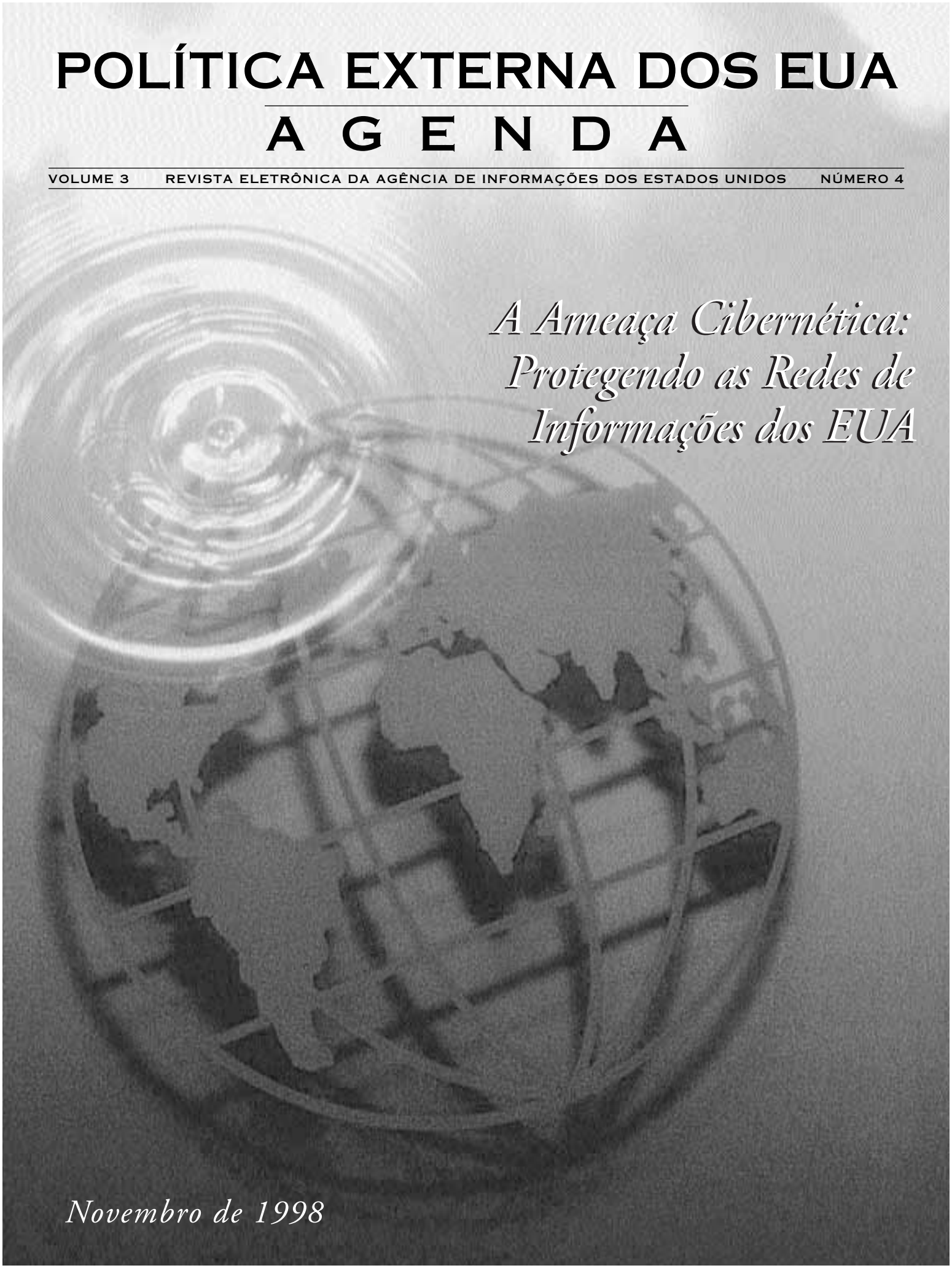
POLÍTICA EXTERNA DOS EUA

AGENDA

VOLUME 3 REVISTA ELETRÔNICA DA AGÊNCIA DE INFORMAÇÕES DOS ESTADOS UNIDOS NÚMERO 4



A Ameaça Cibernética: Protegendo as Redes de Informações dos EUA

Novembro de 1998

POLÍTICA EXTERNA DOS EUA
AGENDA

A Ameaça Cibernética: Protegendo as Redes de Informações dos EUA

AGENDA DE POLÍTICA EXTERNA DOS EUA | REVISTA ELETRÔNICA DA USIA | VOLUME 3 • NÚMERO 4 • NOVEMBRO DE 1998

"Ao nos aproximarmos do século XXI, nossos inimigos ampliaram os campos de batalha – do espaço físico para o espaço cibernético...Em vez de invadir nossas praias ou lançar bombardeiros, esses adversários podem tentar empreender ataques cibernéticos contra os nossos sistemas militares críticos e a nossa base econômica...Se quisermos que nossos filhos cresçam em segurança e liberdade, devemos adotar, em relação a essas novas ameaças do século XXI, o mesmo rigor e determinação que aplicamos aos piores desafios à segurança deste século."

— Presidente Clinton
Discurso por ocasião da formatura de uma turma da Academia Naval dos Estados Unidos
22 de maio de 1998

Esta edição de *Agenda de Política Externa dos EUA* examina a reação dos Estados Unidos a desafios que nunca haviam sido encontrados anteriormente — desafios que só poderiam ocorrer na Era da Informática. Representantes do governo dos Estados Unidos explicam iniciativas que se destinam a proteger as redes de informações dos Estados Unidos contra os ataques cibernéticos e a estimular a cooperação entre os setores público e privado para o desenvolvimento de medidas de segurança. Um senador dos Estados Unidos mostra a reação do Congresso ao debate sobre a guerra da informação, um acadêmico explica a maneira pela qual as universidades estão reagindo às novas prioridades nacionais que estão surgindo, um especialista do setor privado apresenta uma visão geral do significado e da evolução da guerra da informação, e especialistas em segurança do setor privado permitem que se tenha uma visão de como as empresas norte-americanas estão trabalhando em parceria, umas com as outras e com o governo, para fazer frente aos requisitos de segurança da era cibernética.

POLÍTICA EXTERNA DOS EUA

A G E N D A

Uma Revista Eletrônica
da Agência de Informações dos Estados Unidos

A AMEAÇA CIBERNÉTICA: PROTEGENDO AS REDES DE INFORMAÇÕES DOS EUA

ÍNDICE

◉ ÊNFASE

DEFENDENDO A NAÇÃO CONTRA OS ATAQUES CIBERNÉTICOS: A GARANTIA DA INFORMAÇÃO NO AMBIENTE GLOBAL 6
General Kenneth A. Minihan
Diretor da Agência Nacional de Segurança [National Security Agency]

A GARANTIA DA INFORMAÇÃO E A NOVA ERA DA SEGURANÇA 10
BDr. John Hamre
Vice-Secretário de Defesa

CIAO: UMA ABORDAGEM INTEGRADA PARA FAZER FRENTE ÀS AMEAÇAS DE UMA "NOVA ERA" 13
Uma entrevista com o Dr. Jeffrey A. Hunker
Diretor do Escritório de Garantia da Infra-Estrutura Crítica [Critical Infrastructure Assurance Office]

O PROBLEMA DO ANO 2000 18
John Koskinen
Presidente do Conselho Presidencial Para a Conversão do Ano 2000

A AMEAÇA DA GUERRA DA INFORMAÇÃO EXIGE MAIS ATENÇÃO EM TODAS AS FRENTES 20
Uma entrevista com o senador Jon Kyl

◉ COMENTÁRIO

FANTASMAS NAS MÁQUINAS? 24
Dr. Martin Libicki
Analista Político Sênior, RAND

A REAÇÃO DO ENSINO SUPERIOR À GUERRA DA INFORMAÇÃO 28
Dr. Charles W. Reynolds
Diretor do Departamento de Ciência da Computação e Reitor Interino
Faculdade Integrada de Ciência e Tecnologia [College of Integrated Science and Technology]
Universidade James Madison

◉ OPINIÕES DO SETOR PRIVADO

OS SETORES PÚBLICO E PRIVADO SE BENEFICIAM, COMPARTILHANDO CONHECIMENTOS E TÉCNICAS DE SEGURANÇA 33
Uma entrevista com Howard Schmidt
Diretor de Segurança de Informação, Microsoft Corporation

ESTRATÉGIAS PARA FAZER FRENTE ÀS AMEAÇAS AOS RECURSOS DE INFORMÁTICA 36
James A. Lingerfelt
Consultor Sênior da IBM Para Questões de Segurança Pública e Justiça

A GUERRA DA INFORMAÇÃO: DESAFIO E OPORTUNIDADE 43
James Adams
Diretor Geral, Infrastructure Defense, Inc.

INFORMAÇÕES DE CARÁTER GERAL SOBRE A QUESTÃO

FATOS E NÚMEROS: A PROTEÇÃO DA INFRA-ESTRUTURA CRÍTICA DOS ESTADOS UNIDOS 46
Determinação Presidencial N.º 63

SUGESTÕES PARA LEITURA ADICIONAL

A AMEAÇA CIBERNÉTICA: PROTEGENDO AS REDES DE INFORMAÇÃO DOS EUA - NOTIFICAÇÃO SOBRE ARTIGOS 48
Resumos de artigos recentes

A AMEAÇA CIBERNÉTICA: PROTEGENDO AS REDES DE INFORMAÇÃO DOS EUA - BIBLIOGRAPHY 50
Realçando outras opiniões

A AMEAÇA CIBERNÉTICA: PROTEGENDO AS REDES DE INFORMAÇÃO DOS EUA - PRINCIPAIS SITES NA INTERNET 51
Links na Internet, com recursos que tratam de questões relacionadas

POLÍTICA EXTERNA DOS EUA
AGENDA

UMA REVISTA ELETRÔNICA DA AGÊNCIA DE INFORMAÇÕES DOS ESTADOS UNIDOS — VOLUME 3 • NÚMERO 4 • NOVEMBRO DE 1998

As revistas eletrônicas da USIA, publicadas e transmitidas para todo o mundo a cada três semanas, examinam as principais questões enfrentadas pelos Estados Unidos e pela comunidade internacional. As revistas — Perspectivas Econômicas, Questões Globais, Questões de Democracia, Agenda de Política Externa dos EUA, e Sociedade e Valores dos EUA — *apresentam análises, comentários, e informações de caráter geral a respeito das suas áreas temáticas. Todas as edições são publicadas em inglês, francês e espanhol, e alguns números também são publicados em árabe, português e russo.*

As opiniões expressas nas revistas não refletem, necessariamente, as opiniões ou políticas do governo dos Estados Unidos. Favor observar que o USIS não assume nenhuma responsabilidade pelo conteúdo e nem pela continuidade do acesso aos sites da Internet para os quais há links nesta publicação; tal responsabilidade cabe aos respectivos provedores. Os artigos podem ser reproduzidos e traduzidos fora dos Estados Unidos, a não ser que mencionem restrições de copyright.

Números atuais ou atrasados das revistas podem ser encontrados na Home Page da Agência de Informações dos Estados Unidos na World Wide Web, no seguinte endereço:"http://www.usia.gov/journals/journals.htm". As revistas se encontram disponíveis em vários formatos eletrônicos para facilitar a visualização on-line, a transferência, o download, e a impressão. Comentários são bem-vindos no seu escritório local do Serviço de Informações dos Estados Unidos (USIS), ou na redação:

Editor, U.S. Foreign Policy Agenda
Political Security - I/TPS
U.S. Information Agency
301 4th Street, S.W.
Washington, D.C. 20547

E-mail: ejforpol@usia.gov

Favor observar que este número de Agenda de Política Externa dos EUA *pode ser encontrado na Home Page do USIS na World Wide Web, no seguinte endereço: "http://www.usia.gov/journals/itps/1198/ijpe/ijpe1198.htm".*

DEFENDENDO A NAÇÃO CONTRA OS ATAQUES CIBERNÉTICOS: A GARANTIA DA INFORMAÇÃO NO AMBIENTE GLOBAL

General Kenneth A. Minihan

Diretor da Agência Nacional de Segurança [National Security Agency]

A Agência Nacional de Segurança "está usando as suas habilidades especiais para desenvolver a tecnologia fundamental para a criação de uma capacidade nacional de detecção e reação contra ataques cibernéticos," diz o general Kenneth A. Minihan, da Força Aérea dos Estados Unidos. Ele enfatiza o fato de que "a superioridade em informação da Era da Informática é, sem dúvida, um dos principais objetivos do país."

"Estamos correndo riscos. A América depende dos computadores. Eles controlam o fornecimento de energia, as comunicações, a aviação, e os serviços financeiros. Eles são usados para armazenar informações vitais, desde registros médicos até planos de negócios, e incluindo até fichas policiais. Embora confiemos neles, eles são vulneráveis – aos efeitos de projetos deficientes e de um controle de qualidade insuficiente, a acidentes, e talvez o que mais nos preocupa: a ataques intencionais. O ladrão moderno pode roubar mais com um computador do que com uma arma. O terrorista do futuro pode ser capaz de causar mais danos com um teclado do que com uma bomba."

— "Computadores Ameaçados," Conselho Nacional de Pesquisa [National Research Council], 1991

INTRODUÇÃO

Talvez a coisa mais extraordinária a respeito das palavras citadas acima é que elas foram escritas praticamente nos primórdios da Era da Informática. Até recentemente, nós, como nação, demos pouca atenção a elas. Os Estados Unidos, assim como o resto do mundo, continuam a avançar incessantemente para a revolução da informática — a tecnologia da informação está penetrando profundamente no próprio tecido da nossa sociedade, e na nossa economia como nação, na comunidade global. Na verdade, a "Infovia" se tornou a artéria econômica vital da nossa nação.

Os Estados Unidos estão liderando o mundo rumo à Era da Informática, mas também dependem, de maneira extraordinária, da tecnologia da informação — os computadores e a rede global que estabelece as ligações entre eles. Esta dependência se tornou uma ameaça clara e dominante ao nosso bem-estar econômico, à nossa segurança pública, e à nossa segurança nacional.

As redes do mundo, chamadas por muitos de "espaço cibernético", não conhecem limites físicos. Nossa conectividade cada vez maior ao espaço cibernético e através dele, nos expõe cada vez mais aos adversários tradicionais e a um grupo crescente de novos inimigos. Terroristas, grupos radicais, traficantes de drogas, e o crime organizado, podem se unir a nações-estado inimigas, utilizando um enorme arsenal de ferramentas sofisticadas para o ataque informatizado. Os ataques informatizados podem complementar ou substituir os ataques militares tradicionais, complicando enormemente e expandindo as vulnerabilidades que devemos prever e às quais devemos reagir. Os recursos que se encontram ameaçados não incluem somente as informações armazenadas ou que estão sendo transmitidas pelo espaço cibernético, mas todos os componentes da nossa infra-estrutura nacional que dependem da informática e da disponibilidade, em tempo hábil, de dados precisos. Esses componentes incluem a própria infra-estrutura de telecomunicações; os nossos sistemas bancários e financeiros; os sistemas

de energia elétrica; outros sistemas energéticos, como oleodutos e gasodutos; as nossas redes de transporte; sistemas de distribuição de água; sistemas de atendimento médico e serviços de saúde em geral; serviços de emergência, como polícia, bombeiros, e resgate; e atividades relacionadas aos governos de todos os níveis. Todos esses componentes são necessários para que se obtenha o sucesso econômico e para que seja mantida a segurança nacional.

A GARANTIA DA INFORMAÇÃO — OBJETIVO NACIONAL

No dia 22 de maio de 1998, o presidente assinou a Determinação Presidencial 63 [Presidential Decision Directive 63] (PDD-63) sobre a Proteção da Infra-Estrutura Crítica. Nesse documento, ele declara: "Quero que os Estados Unidos tomem todas as medidas necessárias para eliminar, rapidamente, qualquer vulnerabilidade significativa a ataques, tanto físicos quanto cibernéticos, às nossas infra-estruturas críticas, incluindo, especialmente, os nossos sistemas de informática.

O objetivo nacional é o seguinte: no máximo até o ano 2000, os Estados Unidos deverão ter uma capacidade operacional inicial e, no máximo daqui a cinco anos, os Estados Unidos deverão ter e manter a capacidade de proteger as infra-estruturas críticas do nosso país contra atos intencionais que possam comprometer de maneira significativa:

— A capacidade, por parte do governo federal, de cumprir as missões essenciais de segurança nacional e de assegurar a saúde e a segurança do público em geral;
— A capacidade, por parte dos governos estaduais e municipais, de manter a ordem e de prestar os serviços públicos essenciais mínimos;
— A capacidade, por parte do setor privado, de assegurar o funcionamento adequado da economia, e a prestação dos serviços essenciais de telecomunicação, energia, serviços financeiros e de transporte."

Alcançar esse objetivo será uma grande tarefa, que deverá requerer um esforço de cooperação entre os elementos do governo e do setor privado que operam as infra-estruturas críticas. A PDD determina que o governo federal lidere pelo exemplo, assegurando a solidez dos sistemas federais, mas também deixa claro que o setor público não pode resolver o problema de forma unilateral. Todos os departamentos e órgãos do governo federal dependem, e muito, dos serviços prestados pelo setor privado — energia, telecomunicações, transportes, etc. Portanto a PDD tem como objetivo uma Parceria Entre os Setores Público e Privado, que deve desenvolver e implementar um Plano abrangente de Garantia da Infra-Estrutura Nacional, para lidar com a ameaça do terrorismo eletrônico. O desafio significativo é fazer com que o setor privado se envolva na garantia da infra-estrutura, em âmbito nacional. No atual ambiente, em que há muita competitividade, o setor privado, geralmente, é levado a obter vantagens mercadológicas — o que inclui a redução de custos operacionais — para aumentar os lucros. Medidas aperfeiçoadas de proteção cibernética deverão exigir, ao mesmo tempo, maiores investimentos e cooperação com concorrentes.

ELEMENTOS ESSENCIAIS

Qualquer estratégia para realçar a solidez das nossas infra-estruturas críticas deve conter três elementos básicos: maior proteção contra os ataques cibernéticos, a capacidade de detectar um ataque no momento em que ele estiver ocorrendo, e a capacidade de reagir e/ou de se recuperar quando um ataque for detectado.

Uma proteção mais abrangente contra os ataques cibernéticos é baseada em tecnologia de criptografia — incluindo assinaturas digitais — para proporcionar os serviços de autenticação, integridade, não-repudiação, e privacidade/confidencialidade necessários para que as informações sejam asseguradas. Uma sólida autenticação, baseada em assinatura digital usada para proporcionar o controle positivo de acesso, talvez seja a ferramenta mais poderosa para a proteção contra os ataques cibernéticos. A assinatura digital também proporciona integridade das informações eletrônicas e a não-repudiação das transações cibernéticas. A criptografia é utilizada em computadores de mesa, servidores de arquivos, e em redes, para assegurar a privacidade de informações sensíveis de caráter governamental, comercial, e pessoal. A tecnologia de criptografia, que no passado era praticamente uma exclusividade dos governos, atualmente se encontra facilmente disponível no mercado comercial, e é uma das condições fundamentais

para a garantia da informação. Na verdade, no dia 16 de setembro de 1998, o vice-presidente anunciou uma grande atualização da Política de Controle de Exportação dos Estados Unidos a Respeito da Tecnologia de Criptografia [U.S. Export Control Policy on Encryption Technology], uma clara indicação da sua importância para a proteção da infra-estrutura crítica, e também para o comércio eletrônico e para a prosperidade econômica em nível global.

Tendo em vista o amadurecimento da tecnologia de criptografia, o desafio que persiste é a utilização da tecnologia, de forma coerente e eficaz, em todas as nossas infra-estruturas críticas. Isso requer uma estrutura para a utilização dos serviços de criptografia de uma forma escalável, inter-operável, em conjunto com a implantação de uma estrutura de apoio de infra-estrutura de chave pública [public key infrastructure (PKI)], para proporcionar certificados sólidos e reconhecidos em nível global, de assinatura digital e de chave de criptografia, a "carteira de identidade" única, individual, da Era da Informática. No momento, os serviços de PKI estão surgindo no setor privado para atender às necessidades do comércio eletrônico global, e podem ser utilizados como uma alavanca para proporcionar apoio à proteção da infra-estrutura crítica.

Nas áreas de diagnose, detecção e resposta aos ataques cibernéticos, as tecnologias ainda não estão tão amadurecidas ou eficazes. Atualmente, os Estados Unidos possuem pouca capacidade para detectar ou reconhecer um ataque cibernético, seja ele contra as infra-estruturas governamentais ou do setor privado, e menos capacidade ainda para reagir. A capacidade de identificar um ataque cibernético estratégico contra um ou vários componentes da infra-estrutura crítica, e de reagir adequadamente é, sem dúvida, um problema significativo de segurança nacional. Um fator complicador é que as invasões dos computadores têm sido tradicionalmente consideradas como crimes e como "casos de polícia". Quando uma invasão ocorria, o invasor era (assim se esperava) localizado, preso e processado. Além disso, muitas entidades do setor privado relutavam em compartilhar informações sobre invasões dos seus computadores, temendo serem prejudicadas pela imprensa (por exemplo, manchetes de jornal do tipo "Banco Perde Milhões em Invasão de Computador" ou "Hackers Tornam o Serviço de Telefonia Inoperante") e pela reação do público. Para que se possa criar uma capacidade eficaz de defesa cibernética em nível nacional, novas normas de envolvimento precisam ser desenvolvidas, para permitir uma colaboração aberta e dinâmica entre o setor privado, as autoridades policiais, e a comunidade de segurança nacional.

A GARANTIA DA INFORMAÇÃO: UMA NOVA ATRIBUIÇÃO DA AGÊNCIA NACIONAL DE SEGURANÇA

Na Era da Informática, as missões tradicionais da Agência Nacional de Segurança, de Inteligência de Comunicações e Segurança na Área de Informática estão evoluindo no sentido de proporcionar superioridade, no que diz respeito à informação, aos Estados Unidos e seus aliados. Uma parte essencial dessa estrutura é uma profunda compreensão da Infra-Estrutura Global de Informações e das vulnerabilidades dos sistemas de informática em rede aos ataques cibernéticos. Na parte dessa missão referente à defesa, a NSA desenvolveu uma série de iniciativas para proporcionar um arcabouço técnico para proteger as nossas infra-estruturas críticas.

Como mencionamos anteriormente, a tecnologia de criptografia se tornou amplamente disponível no mercado comercial e ela é a base para que se possa proteger os sistemas de informação contra os ataques cibernéticos. O lado ruim é que muitos produtos disponíveis não são compatíveis entre si, sua solidez varia, e há muitas maneiras, freqüentemente confusas, de utilizar a criptografia. Por exemplo, existe criptografia de e-mail, criptografia de arquivos, criptografia da web, criptografia de links, e criptografia de redes virtuais privadas, só para citar alguns tipos. Para remediar a situação, a NSA formou uma parceria com os principais fornecedores de tecnologia de informação provida de segurança, para desenvolver uma estrutura comum para serviços de criptografia, de modo a proporcionar soluções de garantia da informação que possam incorporar toda a indústria. Essa estrutura define uma maneira coerente de aplicar a tecnologia de criptografia à empresa, assim como o meio pelo qual a criptografia interage e apóia outras tecnologias e produtos relacionados à segurança, como por exemplo, "firewalls", servidores, roteadores, sistemas

operacionais, ferramentas para a detecção de invasão, códigos prejudiciais, ferramentas de auditoria, e serviços de infra-estrutura de chave pública.

Outra dimensão do problema é o fato de existirem diferenças na solidez dos muitos produtos associados à segurança, que se encontram disponíveis no mercado. Para tratar dessa questão, a NSA formou uma parceria com o Instituto Nacional de Normas e Tecnologia [National Institute for Standards and Technology] (NIST). Mediante esse acordo, a NSA e o NIST certificarão laboratórios comerciais para avaliar produtos comerciais relacionados à segurança, seja para validar as declarações do fornecedor quanto à segurança, ou para verificar a conformidade com os requisitos da estrutura de segurança da rede. Os testes dos produtos serão feitos pelos laboratórios certificados, que receberão honorários pelos serviços prestados, com o custo e o prazo sendo negociados entre o laboratório e o fornecedor do produto.

Finalizando, a Agência Nacional de Segurança acredita que a nação precisa compartilhar uma série de elementos de garantia de informações referentes à segurança nacional, e está utilizando a sua notável e exclusiva capacidade para desenvolver a tecnologia fundamental para criar uma capacidade, em âmbito nacional, de detectar e reagir a ataques cibernéticos. A abordagem integra uma variedade de sensores que podem ser instalados em pontos críticos da infra-estrutura e na própria infra-estrutura subjacente de telecomunicações, com técnicas analíticas sofisticadas e de ampla escala, para proporcionar uma visão dinâmica das ameaças às infra-estruturas críticas, provenientes do espaço cibernético global. Essas técnicas devem ser compartilhadas por uma série de componentes das áreas federal, industrial, regional e de segurança nacional, para permitir, concomitantemente, a detecção, defesa, reconstituição e recuperação de serviços vitais.

CONCLUSÃO

A prosperidade econômica que a nossa nação desfruta atualmente tem como alicerce, em grande parte, a Era da Informática e a nossa liderança global em tecnologia de informação. A continuidade da nossa liderança e prosperidade na economia global pode depender do nosso compromisso, em nível nacional, no sentido de agir como líderes, trazendo integridade e responsabilidade — garantia de informação — ao ambiente de informação global que ajudamos a criar. O recado do governo — por meio da PDD-63 — é claro: a hora de agir é agora, e a NSA está em posição e preparada para apoiar a iniciativa com o nosso know-how técnico. A superioridade na informação, na Era da Informática, é, sem dúvida, um objetivo nacional da maior importância.

A GARANTIA DA INFORMAÇÃO E A NOVA ERA DA SEGURANÇA

Dr. John Hamre

Vice-Secretário de Defesa

A proteção dos recursos críticos de informação se tornará "um dos mais importantes desafios da segurança nacional dos próximos anos," diz o vice-secretário de Defesa John Hamre. Observando que o Pentágono tem a responsabilidade de proteger 28.000 sistemas diferentes de computadores, ele avisa que a proteção do mundo virtual contra as ameaças cibernéticas "é tanto um processo de abordagem gerencial quanto de tecnologia."

Os Estados Unidos passaram por cinco eras de segurança. Cada uma das mudanças envolveu transições de um passado certo para um futuro incerto. A primeira era foi da Guerra Revolucionária até meados da década de 1820 a 1830. Nesse período, os Estados Unidos se encontravam na margem de um ambiente internacional de segurança que ainda era dominado pela Europa.

De meados da década de 1830 a 1840 até o final do século 19, desfrutamos o isolamento proporcionado pelo Oceano Atlântico e cuidamos das nossas vidas enquanto a velha estrutura política européia se desintegrava. Essa segunda era terminou com a Primeira Guerra Mundial e o surgimento da União Soviética. Uma terceira era transcorreu de 1920 a 1946 e foi caracterizada pela recessão global e pela ascensão do comunismo internacional enquanto a Europa entrava em colapso. Esse eventos determinaram a ocorrência de uma crise para a democracia americana e para o sistema da livre iniciativa, com a Grande Depressão, e as tensões no ambiente de segurança internacional acabaram provocando a eclosão da Segunda Guerra Mundial.

A era mais recente — a Guerra Fria — foi dominada por um mundo bipolar. Os Estados Unidos lideraram a comunidade internacional, criando instituições para reconstruir as economias destroçadas da Europa e lidar com o colapso dos velhos impérios do terceiro mundo, dominados pela Europa. Ao mesmo tempo, os Estados Unidos estavam liderando os estados do mundo livre para conter o comunismo, até o colapso da União Soviética.

Agora estamos na transição para uma nova era, aparentemente caracterizada pela ressurgimento de velhos perigos — nacionalismo e etnicidade. Outra dimensão nessa nova era é a dissolução do controle e a disseminação das tecnologias que foram criadas na era anterior e a dramática ascensão de novos e impressionantes recursos técnicos que apresentam um potencial nunca antes imaginado, para o bem e para o mal. Agora estamos convivendo com o desconcertante temor das "bombas atômicas sem dono" e das armas químicas e biológicas nas mãos de terroristas.

A próxima era da segurança também trará o desafio da segurança cibernética. O crescimento explosivo do uso da informática teve um profundo efeito sobre todos os setores da economia dos Estados Unidos, assim como sobre o governo do país. A informática possibilitou um incrível crescimento econômico, e permitiu que as empresas americanas competissem com uma eficácia nunca antes vista. Os Estados Unidos — assim como o resto do mundo — realmente contam com a informática de uma forma que não se podia imaginar poucos anos atrás.

Isso é particularmente verdadeiro nas forças armadas dos Estados Unidos. O Departamento de Defesa (DOD) está usando a informática para fazer o que chamamos de Revolução nas Questões Militares — a movimentação e a utilização de grande quantidade de informações para proporcionar uma inteligência mais confiável, comando e controle radicalmente aperfeiçoados, melhores práticas comerciais e sistemas de armas mais poderosos. Essa revolução é vital se quisermos continuar prontos para defender os interesses

dos Estados Unidos na atualidade e nos preparar para a evolução das ameaças na próxima era de segurança.

A revolução da informática está atingindo todos os cantos do DOD, tanto no campo quanto na sede. Em breve os nossos soldados em nível de grupo de combate terão comunicações que permitirão aos comandantes saber precisamente a posição, situação e até mesmo os batimentos cardíacos de cada soldado — uma conscientização quase completa em relação ao espaço de batalha. Nossos marinheiros enviam e-mail de seus navios no mar para suas casas usando uma tecnologia muito similar àquela usada na guiagem dos mísseis de cruzeiro. Os pilotos, atualmente, levam em consideração a "saturação de tarefas" do grande fluxo de informações que se encontra à sua disposição em vôo.

Nos nossos processos logísticos, a tecnologia está sendo usada para conectar as linhas de frente às linhas de suprimento. Assumimos o compromisso de ter um processo de aquisição sem papel até a virada do século. Abrimos o nosso Escritório Conjunto de Programação Eletrônica [Joint Electronic Program Office] para simplificar as compras em nível de unidade, e agora estamos usando "shopping centers" eletrônicos baseados na Internet para comprar tudo, de canetas a atuadores hidráulicos. Estamos usando a Internet para um espectro que cobre desde pagamentos de viagens até comunicações por satélite, e temos progredido muito na área de editoração eletrônica.

Resumindo, o DOD está dominando o poder do microchip para construir as forças armadas do século XXI. No entanto, ao fazermos isso, devemos também reconhecer que as novas tecnologias são seguidas por novos perigos. As mesmas tecnologias que nos permitem procurar novas eficiências podem também ser usadas por aqueles que não podem nos atacar no campo de batalha convencional, para nos atacar no espaço cibernético. Isso faz parte de uma dimensão muito diferente e muito importante no pensamento da segurança nacional; as tecnologias que, no passado, somente se encontravam ao alcance das grandes nações-estado, agora estão ao alcance de indivíduos. A proteção dos nossos recursos de informação — a garantia da informação — será, portanto, um dos principais desafios para a segurança nacional nos próximos anos.

Não há dúvida de que a garantia da informação é crítica; nós, do DOD, já vimos a primeira onda de ameaças cibernéticas, tanto em exercícios quanto em ataques reais. Para que pudéssemos ter uma idéia da nossa vulnerabilidade, no ano passado fizemos um exercício. Nosso "inimigo" era um grupo de aproximadamente 35 pessoas cuja missão era invadir os sistemas de computadores do DOD. Suas ferramentas eram limitadas a tecnologias comuns, disponíveis comercialmente, e software que era vendido no mercado ou que podia ser obtido pela Internet, via "download". Dentro de três meses, o grupo, operando com essas restrições, conseguiu nos atacar, invadir nossas redes não-secretas, e na verdade, poderia ter causado sérios danos às nossas comunicações e aos nossos sistemas de energia.

Em fevereiro deste ano, sofremos um ataque organizado contra os sistemas de computadores do Pentágono, no momento em que estávamos aumentando o contingente posicionado no Golfo Pérsico. Descobrimos que os autores do ataque eram dois adolescentes da Califórnia, mas acontecendo quando aconteceu, as suas conseqüências poderiam ter sido muito mais sérias. Tanto o nosso exercício quanto o pequeno ataque serviram como um alerta: a pergunta que deve ser feita quanto aos ataques mais sérios não é "se", mas "quando" e "onde".

Para lidar com essas ameaças, primeiro devemos levar em consideração a nossa mentalidade. Tradicionalmente, os americanos sempre pensaram em segurança como uma cerca no quintal, definindo os limites e protegendo a área demarcada. Se a cerca for danificada, ela pode ser reparada, e o local estará seguro novamente. Essa filosofia funcionava bem nas eras de segurança anteriores, mas não existem fronteiras no espaço cibernético. A transição para a próxima era deverá ser caracterizada não por avanços tecnológicos, mas pela flexibilidade de pensamento. Precisamos nos conscientizar de que a segurança no mundo virtual é tanto um processo de abordagem gerencial e de atenção quanto de tecnologia.

A mudança de mentalidade pode ser uma das tarefas mais difíceis. Sem perceber, por exemplo, estamos, neste exato momento, fornecendo informações a inimigos em potencial, que eles, no passado, gastavam centenas de milhões de dólares em operações de inteligência para obter. Tínhamos uma instalação

militar com o que parecia ser uma excelente home page na Web. A página mostrava uma vista aérea da instalação. Havia legendas identificando os prédios como "Centro de Operações" e "Centro de Apoio Técnico." A página era ótima em termos de relações públicas, mas também fornecia informações valiosas sobre alvos, para aqueles que porventura nos quisessem mal.

Compreendendo as questões mais amplas relacionadas à garantia da informação, devemos agir de modo a tomar providências concretas para proteger os nossos recursos de informática. No ano passado, o DOD concentrou esforços, até então dispersos, para tentar compreender os requisitos para a proteção da nossa infra-estrutura de informática. O ritmo do progresso da área da informática faz com que essa tarefa represente um grande desafio; o DOD possui 28.000 sistemas diferentes de computação, todos sendo atualizados e modificados, e precisamos compreender os seus pontos vulneráveis. O desafio da garantia da informação é como a guerra, e estamos utilizando uma abordagem adequada, alocando um Comandante de Força Tarefa Conjunta Para Defesa de Redes de Computadores para organizar os nossos esforços. O DOD é também um dos principais contribuintes do Centro Nacional de Proteção à Informação [National Information Protection Center] e do Escritório Presidencial de Garantia de Informações Críticas.

Outras providências também se fazem necessárias. Noventa e cinco por cento das nossas comunicações, no momento, se processam por meio de linhas públicas de telefone e fax. Isso faz com que a criptografia seja um elemento-chave na garantia da informação. Um dos cenários mais perigosos no mundo virtual é a possibilidade de nossos combatentes receberem mensagens falsas que os enganariam; portanto, sem uma criptografia confiável, toda a infra-estrutura de informações com a qual contamos se torna vulnerável. Em resposta a essa ameaça, estamos, no momento, trabalhando para garantir que dentro do DOD, possamos garantir a identidade digital dos usuários e desenvolver um sistema confiável de chave pública. Precisamos fortalecer os nossos processos de criptografia, para que as informações que transmitimos e com as quais lidamos eletronicamente sejam seguras e possam ser verificadas.

Além disso, o DOD está evoluindo de maneira significativa no que diz respeito à segurança das redes, em um sentido mais amplo. Estamos instalando a infra-estrutura para a monitoração de redes e estamos trabalhando para garantir o controle de configuração em um ambiente de rede dinâmico e que pela sua própria natureza, está sempre passando por mudanças. Estamos instalando "firewalls" (paredes de fogo), centros de monitoração de redes, assinaturas digitais, e uma infra-estrutura de segurança.

A garantia da informação, a criptografia, e a segurança das redes apresentam alguns dos maiores desafios que o Departamento de Defesa já enfrentou. Para se beneficiar da revolução da informática, devemos garantir o acesso e a proteção aos próprios recursos com os quais contamos. Estamos progredindo rapidamente rumo a esse objetivo, mas muita coisa ainda precisa ser feita. Esta época, que apresenta grandes desafios, requer que contemos com a habilidade dos profissionais de informática, tanto no DOD quanto nas demais áreas do governo e no setor privado, para proteger os sistemas que são vitais para todos nós. Devemos assegurar que o caminho trilhado pela nossa nação rumo à nova era de segurança seja tão bem sucedido quanto foi da última vez

CIAO: UMA ABORDAGEM INTEGRADA PARA FAZER FRENTE ÀS AMEAÇAS DE UMA "NOVA ERA"

Uma entrevista com o Dr. Jeffrey A. Hunker

Diretor do Escritório de Garantia da Infra-Estrutura Crítica [Critical Infrastructure Assurance Office]

"O apoio total do setor privado" é vital para a proteção das infra-estruturas críticas dos Estados Unidos contra os ataques cibernéticos, diz o Dr. Jeffrey A . Hunker, diretor do Escritório de Garantia da Infra-Estrutura Crítica [Critical Infrastructure Assurance Office] (CIAO). "A ameaça que estamos enfrentando está crescendo com o passar do tempo," ele diz. "E portanto, precisamos reagir com uma noção de urgência e produzir resultados reais muito rapidamente para combatê-la." Hunker foi entrevistado pela colaboradora Susan Ellis

Pergunta: Como diretor do CIAO o senhor tem, como atribuição, montar um plano nacional integrado para tratar das ameaças físicas e cibernéticas às infra-estruturas de comunicações, transportes, e energia, assim como outras infra-estruturas críticas da nação. Qual é o principal desafio que o senhor enfrenta ao tratar das suas novas responsabilidades em conformidade com essa iniciativa anunciada pelo presidente Clinton em maio deste ano?

Hunker: O principal desafio que o presidente reconheceu é que, no momento, nós vivemos em uma nova era na qual existem ameaças que nós nunca enfrentamos antes. Mais particularmente, vivemos em uma época em que – devido ao fato de que as telecomunicações e a Internet são tão inter-conectadas com o sistema de energia elétrica, e com os nossos sistemas básicos de transportes e telecomunicações – há uma vulnerabilidade à desestruturação desses sistemas pelo que chamamos de ataque cibernético, usando computadores, usando a Internet para invadir os sistemas e desestruturá-los, torná-los inoperantes. Um ataque desse tipo poderia não apenas interferir, por exemplo com as operações militares, mas poderia também desestruturar quaisquer serviços vitais com os quais a economia conta e com os quais a América conta – como a energia elétrica, o uso da telefonia, e serviços básicos de transporte.

O principal desafio que o presidente reconheceu é que, no momento, nós vivemos em uma nova era na qual existem ameaças que nós nunca enfrentamos antes. Mais particularmente, vivemos em uma época em que – devido ao fato de que as telecomunicações e a Internet são tão inter-conectadas com o sistema de energia elétrica, e com os nossos sistemas básicos de transportes e telecomunicações – há uma vulnerabilidade à desestruturação desses sistemas pelo que chamamos de ataque cibernético, usando computadores, usando a Internet para invadir os sistemas e desestruturá-los, torná-los inoperantes. Um ataque desse tipo poderia não apenas interferir, por exemplo com as operações militares, mas poderia também desestruturar quaisquer serviços vitais com os quais a economia conta e com os quais a América conta – como a energia elétrica, o uso da telefonia, e serviços básicos de transporte.

P: Trata-se de uma coisa completamente nova, não é?

Hunker: Sim. Nos últimos 10 anos nós inter-conectamos os setores econômicos da nação, e isso trouxe grandes benefícios em termos de crescimento econômico e o tipo de prosperidade que a América tem desfrutado. Mas essa nova prosperidade trouxe consigo uma nova vulnerabilidade e – seja quem for que nos queira mal, nações, grupos de terroristas ou cartéis do crime – essa nova vulnerabilidade que acompanha a nossa dependência dos sistemas eletrônicos e dos sistemas de informática é uma nova maneira pela qual podemos ser atacados.

P: Quais são os órgãos do governo que estão envolvidos com o esforço para enfrentar essa ameaça, e de que forma o seu escritório trabalha com eles para cumprir a sua missão?

Hunker: O presidente determinou que 11 grandes órgãos do governo federal trabalhassem em conjunto. Entre os principais, destacamos o Departamento de Defesa e os órgãos a ele associados; a comunidade de inteligência; e os órgãos de segurança – a Polícia Federal americana [Federal Bureau of Investigation], o Serviço Secreto, e o Departamento de Justiça. E eu acho que outros órgãos muito importantes são o Departamento do Comércio e o Departamento de Transportes. A eles foi solicitado que trabalhassem juntos na criação de um plano nacional.

Mas o que é ainda mais importante, eles receberam a incumbência de trabalhar em conjunto com o setor privado. Porque quase todas as infra-estruturas consideradas críticas vulneráveis a ataques pertencem, na verdade, ao setor privado. E se não contarmos com a cooperação e o apoio total do setor privado no desenvolvimento dessa nossa capacidade de auto-proteção, nós não iremos muito longe.

P: Como o senhor avaliará o sucesso da sua missão?

Hunker: Isso é difícil, por se tratar de um novo desafio, e também devido ao fato de que, de muitas maneiras, os tipos de ataques e ameaças contra os quais o presidente nos pediu para proteger a nação estão evoluindo, e são realmente novos. Em alguns casos eles ainda não aconteceram, e medir o sucesso nessa tarefa será difícil. Acho que uma das principais medidas de sucesso será o ponto em que os vários segmentos do setor privado – os proprietários e operadores da malha de energia elétrica, e os nossos setores de transporte, bancário e financeiro – se unirem e, em conjunto com o governo, desenvolverem um plano de ação. Poderemos avaliar a formação dessa parceria dentro de seis meses a um ano. Essa é, realmente, a primeira medida do sucesso.

P: Qual é o prazo que o senhor está tentando cumprir?

Hunker: Temos um prazo curto porque a ameaça que preocupa o presidente – ataques eletrônicos coordenados e sofisticados contra as infra-estruturas críticas da nação – já existe. O presidente pediu que criássemos um plano nacional com uma capacidade inicial de proteção contra os novos tipos de ataques cibernéticos até o ano 2000. E ele pediu que até o ano 2003, tivéssemos total capacidade operacional para proteger a nação. A ameaça que estamos enfrentando está crescendo à medida que o tempo passa. E portanto precisamos responder urgentemente e produzir resultados de verdade, muito rapidamente, para combatê-la.

P: Estou ciente de que o senhor pretende ter alguma coisa pronta até novembro.

Hunker: É verdade. De fato, uma das primeiras providências que o presidente pediu no pronunciamento que fez em maio, é que dentro de seis meses, o que quer dizer em meados de novembro, os órgãos do governo federal deverão ter feito um trabalho significativo no sentido de desenvolver seus próprios planos para proteger as suas próprias infra-estruturas críticas. Isso significa que, entre outras coisas, o Departamento do Tesouro e o Departamento de Defesa terão um processo para estabelecer defesas para se protegerem contra ataques eletrônicos. Em segundo lugar, o presidente pediu que determinássemos as etapas de um plano nacional, maior, que envolverá uma estreita colaboração com o setor privado, integrando o trabalho de vários órgãos, e incorporando as comunidades acadêmica e de pesquisa, e outros grupos similares, para que haja muitos elementos diferentes. O plano nacional não estará pronto em novembro, mas até lá teremos estabelecido etapas importantes no sentido de construir esse plano nacional.

P: Como o senhor avaliaria a natureza e a gravidade dos ataques às infra-estruturas críticas dos Estados Unidos, e quais são os setores mais vulneráveis?

Hunker: Para entender a ameaça às infra-estruturas críticas dos Estados Unidos, e vulnerabilidade dessas infra-estruturas, precisamos, antes de mais nada, entender a maneira pela qual a economia vem se desenvolvendo. No decorrer dos últimos dois anos, com o crescimento da Internet, cuja utilização e tamanho têm dobrado a cada 10 meses, serviços vitais com os quais os americanos contam – coisas como a energia elétrica, o nosso sistema bancário, o nosso sistema de telecomunicações – estão todos inter-conectados. Esses sistemas são a base para o crescimento econômico e para o apoio a missões vitais para a segurança nacional, e no momento, eles estão muito vulneráveis.

Tivemos uma ocorrência no início deste ano em que,

durante a concentração de forças em resposta às ações do Iraque, tivemos indicações de que "hackers" estavam penetrando em sensíveis computadores do Departamento de Defesa. Essa preocupação ocupou os mais altos níveis do governo durante várias semanas, enquanto o nosso pessoal examinava as fontes desse ataque. Ele se originava do Iraque ou de seus aliados? Finalmente descobriu-se que os ataques eram da autoria de dois "hackers" adolescentes, nos Estados Unidos, apoiados por alguém, em outro país, que os orientava. Mas isso lhe dá uma idéia de como somos vulneráveis.

Um outro hacker adolescente de Massachusetts tornou inoperante uma grande parte da rede de telefonia de Massachusetts, e ao fazer isso, fez com que um grande aeroporto ficasse eletronicamente "cego" por algum tempo, causando ameaças reais à segurança do tráfego aéreo. Se hackers isolados podem causar esse tipo de dano, imagine o que um ataque sofisticado, organizado, que tenha sido projetado para tornar inoperantes partes significativas do nosso sistema de energia elétrica ou de telecomunicações, ou para entrar em computadores sensíveis, poderia fazer. Essa é a natureza da ameaça que estamos enfrentando. E existem muitas indicações segundo as quais pessoas em outros países estão cientes, e estão desenvolvendo esse tipo de capacidade ofensiva para atacar os Estados Unidos eletronicamente.

P: Como diretor do CIAO, o senhor está coordenando um programa nacional de educação e conscientização. Qual é a sua mensagem e como o senhor está transmitindo essa mensagem para os cidadãos dos Estados Unidos?

Hunker: É muito importante que, ao falarmos sobre educação e conscientização, consideremos duas mensagens diferentes. Uma é a conscientização. Estamos lidando com uma nova era, e esse é um novo tipo de ameaça que apenas recentemente se tornou motivo de grande preocupação. Portanto a conscientização, sem dúvida, faz parte da mensagem. No entanto, tenho me sentido muito feliz, porque – ao falar com pessoas de todos os setores do governo em nível ministerial, bem como funcionários de alto nível – as pessoas compreendem a natureza da ameaça. E os nossos principais líderes empresariais e acadêmicos também compreendem isso.

A nossa segunda mensagem é: o que podemos fazer sobre isso? E é por isso que estamos construindo a parceria entre a iniciativa privada e os vários setores do governo, para agir de verdade nos próximos meses, e, em seguida, obviamente, nos anos seguintes, para reagir a isso.

P: Como o senhor descreve a extensão em que nos tornamos dependentes dos computadores, não apenas na nossa vida particular mas para o funcionamento básico da nossa sociedade?

Hunker: Dê uma olhada na sua casa ou em qualquer escritório que você use. O que você vê é a nossa dependência dos sistemas eletrônicos. Vamos ao banco e usamos uma caixa automática; trata-se de um sistema eletrônico que está inter-conectado em nível nacional e internacional. Nossa rede de energia elétrica está, cada vez mais, sendo administrada, na verdade, usando a Internet. A aviação e a rede ferroviária também dependem de sistemas eletrônicos. Até mesmo as empresas que você não considera empresas de computação ou de software – suas operações e produtividade dependem de sistemas de informática que são inter-conectados.

Estima-se que entre um terço e a metade do crescimento econômico que ocorreu neste país nos últimos dois anos, com a criação de milhares de empregos, tem sua origem no comércio eletrônico. Esta é a base do nosso crescimento econômico no futuro; é também a base para o apoio à nossa missão de segurança nacional, seja movendo material e pessoal pelo mundo, ou seja coletando informações vitais e inteligência a respeito de ameaças. Tudo isso tem como base esses novos sistemas eletrônicos.

P. De que forma os senhores estão trabalhando em conjunto com as áreas comercial e industrial do setor privado para reforçar a proteção às redes de informação e comunicação dos Estados Unidos?

Hunker: A estreita colaboração com o setor privado é, de fato, essencial para o atingimento da nossa meta e para a missão definida pelo presidente. O que vou dizer agora pode ser uma coisa apócrifa, mas com certeza 90 a 95 por cento dos sistemas de comunicação do Departamento de Defesa são de propriedade do setor privado e por ele operados. Isso é vital. Se não conseguirmos envolver o setor privado, não iremos

muito longe.

No momento estou participando de uma série de reuniões com outros funcionários de alto nível, de vários departamentos do governo – incluindo o Departamento do Tesouro e o Departamento de Transportes – e com líderes do setor privado que atuam nos setores de infra-estrutura crítica dos sistemas bancário e de transportes, por exemplo. Essas reuniões fazem parte do esforço de cooperação para construir a parceria entre o governo e o setor privado.

Em setembro eu estive em Charlotte, Carolina do Norte, em uma reunião com o prefeito e outras autoridades locais, além de diretores de alguns bancos de grande porte. Charlotte é o segundo centro de atividade bancária do país. E a finalidade da minha visita era assegurar que os principais bancos em Charlotte fizessem parte da parceria.

Temos planos para uma série de reuniões, mais tarde, neste outono, que envolverão o presidente, o vice-presidente, e o assessor de segurança nacional, assim como os líderes dos setores energético, bancário, financeiro, de transportes e de outras infra-estruturas críticas, para dar prosseguimento à construção dessa parceria.

Trata-se de um longo processo. A construção de parcerias, particularmente em uma área na qual nunca tínhamos trabalhado juntos antes, não acontece da noite para o dia. No entanto, estou muito satisfeito com o tipo de resposta e conscientização, e cooperação de verdade que tenho visto, da parte de diretores, presidentes, e outros altos executivos de todas empresas com as quais tenho trabalhado.

P: O CIAO está envolvido com comunidades universitárias e programas para ajudar a encontrar melhores maneiras de proteger a infra-estrutura de informática e outras infra-estruturas críticas dos Estados Unidos?

Hunker: A comunidade acadêmica será uma outra parte importante do tipo de parceria com a qual estamos lidando. Na verdade, em setembro, eu me encontrei pessoalmente com os reitores e diretores de várias universidades de grande porte – a Universidade da Carolina do Norte, Universidade Purdue, o Instituto de Tecnologia de Massachusetts, a Universidade de Virginia, para mencionar somente algumas. Temos dois motivos para isso. Nesse momento, no país, temos uma carência de especialistas em computadores e informática. E a ameaça de ataques cibernéticos simplesmente vai agravar a carência que estamos enfrentando. Ela causará um aumento na demanda de pessoas que possuem treinamento na área. E as universidades serão a linha de frente para o treinamento dos tipos de pessoas das quais vamos precisar.

Também vamos precisar do tipo de pesquisa e desenvolvimento que desenvolverá novas soluções, e que desenvolverá novas tecnologias para proteger os nossos sistemas de informática. E as universidades serão uma parte essencial desse esforço.

P: Como diretor do CIAO, o senhor tem a responsabilidade de desenvolver iniciativas no legislativo. De que maneira o senhor está interagindo com o Congresso dos Estados Unidos e como o senhor avalia o impacto do Congresso sobre as políticas e estratégias relacionadas aos objetivos do CIAO?

Hunker: O trabalho junto ao Congresso é uma parte muito importante desta agenda. E eu diria que o interesse por parte do Congresso tem sido muito grande, e que o Congresso tem nos dado muito apoio quando se trata de reagir a essa nova forma de ameaça terrorista ou ameaça à segurança nacional. Eu posso prever que continuaremos a trabalhar em conjunto com o Congresso em várias questões, e sem dúvida, no que se refere a recursos.

Como parte do trabalho que estamos fazendo, estamos prevendo que o presidente incluirá no seu orçamento para o exercício do ano 2000 uma grande iniciativa para a proteção das infra-estruturas críticas. Isso incluirá recursos para pesquisa e desenvolvimento; incluirá recursos para novas iniciativas para treinar especialistas em informática, tanto para o governo federal quanto para o setor privado, e talvez outras iniciativas. Portanto, o apoio sob o ponto de vista de recursos será muito importante.

Além disso o Congresso examinará as leis atuais que tratam da segurança dos computadores. Freqüentemente, um "hacker" passa por vários computadores até chegar, finalmente, ao computador

que realmente deseja invadir. De acordo com a legislação atual, se você quiser rastrear o caminho trilhado pelo "hacker" – e se ele tiver passado por vários estados – você precisa obter mandados de busca com juízes do país inteiro para poder executar esse trabalho. Estaremos trabalhando em estreita colaboração com o Congresso para examinar os tipos de procedimentos e proteções legais que existem atualmente

P: O senhor acha que há necessidade de maior colaboração e cooperação internacional para a proteção de infra-estruturas chaves? Se este é o caso, de que maneira isso pode ser conseguido?

HUNKER: O aspecto internacional está presente em tudo que se relaciona ao mundo cibernético. Estamos falando de uma ameaça que pode vir do exterior; ela pode vir também do nosso próprio país. Mas esse tipo de ameaça não requer que as pessoas estejam próximas das instituições ou da infra-estrutura que estão atacando.

No ano passado tivemos uma situação em que um hacker na Alemanha, que era, na verdade, um cidadão indiano, estava invadindo um sistema financeiro em Miami, para tentar fazer uma extorsão. Portanto, temos dois países e os cidadãos de três países, essencialmente envolvidos em um incidente que era um ataque direto a uma instituição dos Estados Unidos. Isso lhe dá um pequeno exemplo das implicações internacionais de tudo isso.

A Comissão Presidencial Sobre a Proteção da Infra-Estrutura Crítica emitiu o seu relatório no ano passado, depois de analisar o assunto durante dois anos. Suas recomendações foram fundamentais para a base da iniciativa que o presidente anunciou em maio. A comissão reconheceu que a dimensão internacional é muito importante.

O presidente determinou que o Departamento de Estado assumisse a liderança nas nossas discussões com outros países no que diz respeito a compartilhar informações e ao potencial para novos tratados ou protocolos para reagir aos tipos de ataques terroristas, ou a outros tipos de ataques que poderiam ocorrer. Vários países já manifestaram interesse nisso. Já compareci, pessoalmente, a reuniões com representantes dos governos do Canadá e do México, e estou ciente de que têm ocorrido discussões no contexto da OTAN e outras organizações internacionais sobre esta questão.

Portanto, há muito interesse, mas ainda estamos começando a trabalhar, em relação à maneira pela qual a agenda internacional deverá se desenvolver.

Outra questão importante é a sobreposição entre o trabalho visando a proteção contra ataques cibernéticos – sejam eles oriundos do crime organizado ou de grupos terroristas, ou de outras nações – e aquilo que se convencionou chamar de bug do milênio (Y2K), o problema dos computadores com o ano 2000. O Y2K é diferente porque sabemos exatamente quando o problema vai acontecer. E trata-se de uma coisa que nós mesmos fizemos, porque, há anos, os programadores de computador não levaram em consideração o fato de que a ano 2000 teria um conjunto de datas diferentes daquele do ano 1900. (Muitos sistemas de computação mais antigos usam somente os dois últimos dígitos de um ano para acompanhar a data.)

Mas, sob muitos aspectos, lidar com a ameaça do Y2K requer as mesmas providências que se fazem necessárias para nos protegermos contra os ataques cibernéticos. A primeira coisa que as instituições, as empresas, e o governo federal têm que fazer é identificar os sistemas que possuem e como eles estão inter-conectados, e em seguida eles terão que determinar os sistemas cuja proteção tem prioridade, e como protegê-los.

Outro aspecto do problema do ano 2000 que se sobrepõe ao problema dos ataques cibernéticos é a criação de uma capacidade nacional de reagir e reconstruir sistemas, se alguma coisa errada acontecer no ano 2000. Este também será o modelo para uma capacidade nacional para reagir aos ataques cibernéticos. Tal capacidade envolverá as principais atividades, os meios de reação em nível estadual e municipal, e as principais áreas do governo federal. E, na verdade, o meu escritório trabalha em estreita colaboração com John Koskinen, o assessor especial do presidente para questões referentes ao ano 2000, em vários aspectos desta agenda que se sobrepõem, incluindo as questões do Y2K e os ataques cibernéticos.

O PROBLEMA DO ANO 2000

John Koskinen

Presidente do Conselho Presidencial Para a Conversão do Ano 2000

A pessoa encarregada de liderar o esforço do governo dos Estados Unidos para lidar com o problema dos computadores no ano 2000 diz que o principal obstáculo a ser vencido é a "conscientização insuficiente" sobre o problema "entre os líderes governamentais, jornalistas, executivos das empresas, e o público em geral" no mundo inteiro. Ele teme que a "inatividade e o desconhecimento possam resultar na ocorrência das piores situações possíveis." Mas ele ressalta que "agindo agora podemos minimizar os problemas, e ter a esperança de que a passagem para o ano 2000 transcorra sem maiores dificuldades."

Atualmente o mundo está enfrentando um dos maiores desafios da Era da Informática. Ao nos aproximarmos do novo milênio, muitos sistemas de computação, assim como os chips de computador embutidos em tudo, desde computadores pessoais até aparelhos electrodomésticos e equipamentos industriais sofisticados, estão programados para recuar no tempo.

O problema é que muitos sistemas de computação e microprocessadores – como os chips de computadores são conhecidos - mais antigos, somente usam os dois últimos dígitos de um ano para indicar a data. Portanto, com a chegada do ano 2000, esses chips podem reconhecer 00 como o ano 1900, em vez de 2000. Os problemas funcionais daí resultantes podem causar sérias desestruturações nas malhas energéticas, estações de tratamento de água, redes de serviços financeiros, sistemas de telecomunicações, e sistemas de controle de tráfego aéreo no mundo inteiro. Em um mundo cada vez mais inter-conectado, com uma economia global, as redes de computadores são apenas tão fortes quanto o seu elo mais fraco. Embora cada nação provavelmente tenha os seus próprios problemas particulares com os seus sistemas, nós todos estamos nisso juntos, literalmente.

Por que os projetistas de software cometeram um erro tão óbvio? Trinta anos atrás havia muito menos memória de computador disponível do que hoje, e portanto os programadores de computador contavam com atalhos como o ano de dois dígitos para economizar memória. Eles partiam da premissa de que os programas que projetaram estariam obsoletos e seriam substituídos por novo software muito antes do ano 2000. Na prática, contudo, muitos sistemas de computação grandes e complicados, como os que são utilizados por bancos, empresas de seguros, e corretoras de valores, evoluíram com o tempo, e os softwares mais modernos foram acrescentados aos sistemas existentes. Conseqüentemente, qualquer organização que opere sistemas de computação inter-conectados, em grande escala, terá que verificar milhões de linhas de código de computador para determinar como o sistema trata as datas, em seguida reescrever software para corrigir o problema, executar esses aplicativos para ver como eles funcionam, e depois verificar a interface de cada programa com os aplicativos internos e externos que ele usa.

O reparo tecnológico não é difícil, mas devido à gravidade dos problemas do ano 2000, estamos enfrentando um enorme desafio organizacional e gerencial. Só para citar um exemplo – o contingente de mão-de-obra qualificada para resolver o problema é limitado; trata-se de programadores peritos em linguagens de computação que podem ter se tornado obsoletas anos atrás.

Para coordenar o trabalho referente a esse problema nos muitos sistemas do governo dos Estados Unidos, o presidente Clinton formou um conselho de mais de 30 órgãos. O nosso primeiro objetivo é manter os serviços básicos do governo – assegurar que os benefícios de atendimento médico e de desemprego continuem sendo pagos, e que a coleta dos impostos não seja desestruturada. O ambicioso alvo do presidente é fazer com que 100% dos sistemas do governo dos Estados Unidos estejam em conformidade em relação ao

"problema do ano 2000" – isto é – o problema deverá estar resolvido – até março de 1999. O conselho também possui grupos de trabalho dedicados à interação com os governos estaduais e locais no que diz respeito a esse problema, e a avaliar os esforços das empresas privadas em 35 segmentos de atividade, como transporte, telecomunicações, e finanças.

Além disso, estamos preocupados com a situação dos esforços referentes ao ano 2000 nos outros países, pois muitos sistemas de computação atravessam fronteiras e, em uma economia globalizada, nenhuma nação é uma ilha digital. Estamos trabalhando, por meio de órgãos internacionais, para tratar do problema. A Organização das Nações Unidas aprovou uma resolução segundo a qual todos os países membros deveriam agir e se reportar à Assembléia Geral até 1º de outubro. O Banco Mundial realizou 20 conferências regionais para promover a conscientização no que se refere a essa questão. O Fundo Monetário Internacional concordou em usar a sua influência para dedicar recursos a esse problema. A secretária de Estado Madeleine Albright enviou uma mensagem às embaixadas dos Estados Unidos no mundo inteiro, instruindo os embaixadores para que eles verificassem, em cada país hospedeiro, em que nível se encontravam a preparação para o ano 2000. A Agência de Informações dos Estados Unidos lidera um grupo do Conselho Presidencial, cuja missão é promover a conscientização, agir como via de acesso à informação, e se concentrar nos planos de contingência com outros países.

Infelizmente, agora que faltam menos de 500 dias para chegarmos a 1o de janeiro de 2000, eu acho que o maior problema ainda é a conscientização insuficiente entre os líderes governamentais, jornalistas, executivos de empresas, e o público em geral, em muitos países. A primeira etapa é a seguinte: as nações e as empresas privadas precisam fazer um levantamento de todas as suas operações que envolvem computadores e desenvolver um plano para corrigir o problema. Uma segunda etapa essencial é o planejamento de contingência. O Conselho Presidencial Para o Ano 2000 pediu a cada órgão do governo dos Estados Unidos que desenvolvesse dois tipos de planos; um deles é: o que faremos se um dos nossos sistemas de computação não funcionarem? O segundo nível é o planejamento para contingências externas: o que faremos se os sistemas inter-conectados aos nossos sistemas falharem?

Os problemas referentes ao ano 2000 provavelmente começarão a aparecer antes do novo milênio, à medida que os sistemas obsoletos começarem a calcular ou programar eventos futuros. No momento é difícil prever com exatidão o que vai acontecer. Existem alguns sites na Web nos Estados Unidos nos quais alguns peritos, que normalmente seriam chamados de alarmistas, previram falhas generalizadas em sistemas que resultarão em interrupções no fornecimento de energia elétrica, problemas de tráfego, recessão econômica, e possivelmente, em algumas regiões, escassez de alimentos. Embora eu tenha uma tendência a ser mais otimista do que esses mensageiros da desgraça, estou particularmente preocupado com os países onde a inatividade e a falta de conscientização podem resultar na concretização das piores previsões possíveis. A questão é: agindo agora podemos minimizar os problemas, e podemos ter a esperança de que a transição para o ano 2000 ocorra sem traumas.

A AMEAÇA DA GUERRA DA INFORMAÇÃO EXIGE MAIS ATENÇÃO EM TODAS AS FRENTES

Uma entrevista com o senador Jon Kyl

Nem o governo, nem o Congresso, nem o público em geral está dando atenção suficiente — e nem levando a sério — à crescente ameaça da guerra da informação, diz o senador Jon Kyl. Os adversários em potencial estão aperfeiçoando a sua capacidade de atacar a infra-estrutura crítica, que é responsável, cada vez mais, pela operação dos sistemas de comunicações, transportes e finanças da nação — assim como o seu sistema essencial de defesa, ele avisa. Kyl, republicano do Arizona, é o presidente da Subcomissão, da Comissão Judiciária do Senado, Para Questões Referentes à Tecnologia, Terrorismo e Informações Governamentais. Ele também é membro da Comissão Selecionada do Senado Para Questões de Inteligência. Kyl foi entrevistado pelo colaborador Ralph Dannheisser.

Pergunta: Em uma audiência da comissão, em junho, o senhor disse que o "frágil ventre digital" dos Estados Unidos se encontra mais prontamente vulnerável a um ataque do que as forças armadas da nação. O senhor pode falar um pouco mais sobre isso?

Kyl: Acho que isso geralmente é reconhecido como verdadeiro. Temos o complexo militar mais forte do mundo, e ninguém, de fato, tem condições de nos enfrentar. Portanto, a pergunta é: um adversário em potencial procuraria os pontos mais vulneráveis para atacar os Estados Unidos, caso se decidisse a fazê-lo? A mesma coisa acontece com os terroristas. E a resposta é que uma das nossas vulnerabilidades é a nossa infra-estrutura de informações, porque contamos, mais do que qualquer outra nação do mundo, com a alta tecnologia, para operar as nossas telecomunicações, os nossos transportes, para fazer os nossos negócios financeiros — incluindo, naturalmente, o nosso complexo de defesa. Como resultado, a vulnerabilidade que a nossa infra-estrutura tem é provavelmente um dos principais pontos-alvo para um estado agressor ou uma organização terrorista.

P: Seguindo essa mesma linha de raciocínio, o senhor disse que essa é a mais difícil e mais importante questão de segurança nacional e ordem pública que a liderança do nosso país enfrentará nos próximos anos. Quais são algumas das coisas que o senhor teme como as piores situações possíveis, se essa questão não for tratada adequadamente?

Kyl: Vamos começar com a transição para o novo milênio. O problema do Y2K (problema dos computadores com o ano 2000) que foi — acertadamente — identificado como um sério problema em potencial para o país, é exacerbado pelo fato de que ele dará aos terroristas, ou outros grupos de pessoas ou indivíduos que nos queiram mal, a oportunidade de ouro de atacar no momento em que a maior confusão reinar. Nós não saberemos o motivo pelo qual muitas coisas que vão apresentar problemas à meia-noite de 31 de dezembro de 1999, vão, de fato, ter problemas. Possivelmente atribuiremos a maior parte dos problemas às panes associadas ao Y2K, mas é obvio que essa situação representa uma grande oportunidade para sabotagem ou outro tipo de ataque à nossa infra-estrutura, por parte das pessoas que querem nos prejudicar — tanto pelo fato de suas atividades serem cobertas pelo evento quanto devido à vulnerabilidade que o evento propriamente dito apresenta.

Portanto, aí está a primeira grande oportunidade. Mas além desse momento — devido, como eu disse, à vulnerabilidade dos vários aspectos da nossa sociedade civil, assim como de certos componentes de defesa — o ato de atacar a nossa infra-estrutura representa uma das melhores maneiras de nos prejudicar sob o ponto de vista abstrato, e em uma situação em que haja um conflito contínuo, representa uma grande oportunidade de desestruturar a nossa capacidade de enfrentar as ameaças envolvidas nessa contingência.

P: De modo geral, com que facilidade se pode invadir a rede de informações em algum ponto, e que tipo de

danos a pessoa que conseguir fazer isso pode causar?

Kyl: Bem, é surpreendentemente fácil. É difícil quantificar em palavras, mas alguns exercícios foram feitos recentemente. Um deles, que foi divulgado pela imprensa, chamado "Elegible Receiver" [Receptor Autorizado], demonstrou em termos reais a vulnerabilidade da rede de transportes, da rede de energia elétrica, e outras, aos ataques, literalmente, perpetrados pelos hackers — pessoas usando equipamentos convencionais, em outras palavras, nenhum equipamento de "agente secreto". Os equipamentos que se encontram disponíveis podem nocautear partes essenciais da nossa infra-estrutura de informações. Agora, nesse caso, eles tornaram inoperantes partes da rede elétrica, do sistema de transportes, do sistema financeiro. Outros que são vulneráveis incluem coisas como os sistemas de água, todas as formas de telecomunicações, naturalmente, e as pessoas que atendem às emergências, mas talvez sob o ponto de vista de defesa, nada seja mais sério do que os laboratórios do complexo de defesa, assim como os sistemas de armamento.

Portanto, existe um alto grau de vulnerabilidade, e cada vez que algum jovem hacker de outro país invade o sistema de computadores do Pentágono, as pessoas coçam suas cabeças e se perguntam como isso pode acontecer, e aprendem a partir da experiência. Mas parece que se trata de um processo de aprendizado constante. Outro exemplo: pouco antes do confronto, em fevereiro último, em que estávamos prestes a tomar uma atitude contra Saddam Hussein, a invasão dos computadores do Pentágono foi tão significativa que o presidente foi, de fato, informado de que a atividade poderia ser o resultado de uma ação deliberada por parte do governo do Iraque. Por algum tempo ficamos sem saber se essa foi ou não a causa do ataque. Acabamos descobrindo que o ataque foi perpetrado por três jovens em três países diferentes. Portanto, respondendo à pergunta — "Até que ponto somos vulneráveis?" Eu acho que isso serve como exemplo da questão.

P: Certamente, como esses jovens sem nenhum motivo sinistro podem entrar nos sistemas com tanta facilidade, o senhor sugeriria que os nossos adversários poderiam fazer a mesma coisa com a mesma facilidade, com uma possibilidade muito maior de causar danos?

Kyl: Isso é exatamente o que é preocupante.

P: A partir da sua própria perspectiva no comitê e estando muito interessado no assunto, como o senhor vê o papel do Congresso na proteção contra esse tipo de guerra de informações ou terrorismo cibernético?

Kyl: Bem, acho que é óbvio — temos que dar aos órgãos responsáveis pela segurança nacional, as instituições de defesa, dinheiro suficiente para que eles possam lidar com o problema, e a autoridade para fazê-lo.
Há muitas questões reais envolvidas, mas eu acho que sob o ponto de vista de política pública, precisamos, antes de mais nada, estabelecer a política para o governo, levar essa política a sério, e prover os meios para isso.

Agora, estamos pressionando o governo (Clinton) há quatro anos, e ele ainda está atrasado. Ele deveria apresentar um plano, mas ainda não fez isso. O que o presidente fez, em uma ordem executiva, foi estabelecer um prazo de 180 dias para que um plano fosse preparado. O dia 22 de novembro seria o término do prazo. Portanto, presume-se que esse é o plano dos órgãos do governo para tratar da questão entre si.

P: Isso aconteceu por insistência do Congresso?

Kyl: O Congresso deu o pontapé inicial, pedindo, ou exigindo, duas vezes, que o presidente apresentasse um plano ou um relatório. Ele não fez isso. Em vez disso, ele instituiu uma comissão, antes de mais nada, e como parte dessa iniciativa, ele também instituiu uma força-tarefa dentro do governo. Uma das recomendações que elas fizeram foi para preparar esse plano. E portanto, há muito tempo que eles estão fazendo planos para começar o início da apresentação do relatório, aqui, e já estamos quase no fim processo de 180 dias. Espero que esse plano pelo menos indique a direção a seguir para cada órgão-chave do governo, ao lidar com o setor privado com o qual eles têm um relacionamento, e que proporcione uma orientação, pelo menos para a primeira fase da atividade. Mas ainda falta uma parte significativa do componente de defesa, que é onde eu acho que o governo vai ter que se empenhar a seguir. Portanto, o nosso papel, eu acho, é continuar a pressionar e a prover quaisquer recursos que se fizerem necessários.

P: O senhor acha que a questão está obtendo a atenção necessária, por parte do poder legislativo, para essa finalidade?

KYL: Não. Mas não tem havido desacordo no poder legislativo. Está sendo feito um esforço bipartidário e bicameral. Portanto, nessa área, não há problema. Mas se você perguntar — "Há compreensão suficiente da questão, por parte do Congresso ou do público em geral?" — a resposta é "Não." E também não há compreensão e nem comprometimento suficiente, por parte do governo.

P: O senhor tocou levemente neste assunto, mas devido à interconexão da infra-estrutura de informações, existe uma necessidade, por parte dos setores público e privado, de coordenar, de alguma forma, as suas atividades nessa área e trabalhar em conjunto?

KYL: Sim, existe. E parte do plano que prevemos que o governo desenvolverá é lidar com esse elemento de coordenação. Por exemplo, o Departamento dos Transportes, presumivelmente, terá um plano que integre os componentes da atividade de transportes, que pertencem ao setor privado, ao Departamento de Transportes, para uma reação conjunta — indicações, advertência e reação — etc. Existe também um grupo empresarial que tem estado envolvido, principalmente com a área de telecomunicações, que tem tido uma ligação de longo prazo com o presidente. Os elementos desse grupo continuam a dar muitas indicações sobre o que o setor privado precisa, e o que eles podem fazer para lidar com essa situação. Porque em última análise, o equipamento e a tecnologia gerados pelo setor privado acabam sendo usados tanto pelo setor privado quanto pelo governo, e eles podem ser muito inovadores no que diz respeito ao que eles incorporam aos seus sistemas e como eles oferecem soluções para o governo. Isso é o que eles têm feito.

P: O senhor mencionou anteriormente uma suspeita a certa altura dos acontecimentos, que, segundo se provou, era infundada, de que o Iraque estava empreendendo alguma atividade na área da guerra de informação. O senhor sabe de algum, ou mais de um, adversário dos Estados Unidos que esteja, de fato, se envolvendo com esse tipo de preparação, e qual seria a natureza dessa preparação?

KYL: De acordo com as nossas fontes de inteligência, muitos países estão trabalhando em técnicas de guerra de informação, e há um grupo menor de países que, especificamente, escolheu os Estados Unidos como alvo nos seus esforços de planejamento. Não posso dizer se já houve alguma tentativa, por parte de outro país, de atacar a nossa infra-estrutura de informação.

P: Acho que os ataques ocorreriam de duas formas: Atingindo, de fato, certas áreas de atividade que são controladas pelo sistema de informação, ou inserindo informações falsas nos sistemas.

KYL: Você poderia invadir e adquirir informações, você poderia inserir vários tipos de "bugs" que desorganizariam as operações ou impediriam o seu funcionamento, ou inserir informações falsas. Portanto, na verdade, você poderia fazer todas essas três coisas.

P: E presumivelmente, alguém em algum lugar deve estar pelo menos pensando em fazer isso.

KYL: Como eu disse, muitos países têm programas em andamento, e alguns desses programas, na verdade, têm os Estados Unidos como alvo. Agora, isso não é a mesma coisa que dizer que esses países estão tentando atacar os Estados Unidos hoje. Eu estou apenas dizendo que eles desenvolveram programas, ou que estão trabalhando no conceito de guerra de informações contra os Estados Unidos. Seria óbvio, e essa talvez seja a sua próxima pergunta, que os Estados Unidos estariam pensando em termos tanto ofensivos quanto defensivos.

P: O senhor poderia falar um pouco mais sobre isso?

KYL: A única coisa a mais que eu posso dizer é o seguinte: devo lembrar os nossos leitores que, naturalmente, com relação à capacidade de empreender uma guerra de informação ofensiva, nós somos, de longe, o país mais vulnerável, por causa do nosso grau de dependência da tecnologia; portanto, para nós trata-se mais de uma atividade defensiva do que uma atividade ofensiva.

P: Mas o senhor está sugerindo que certamente há

também preparações ou investigações em andamento.

KYL: Bem, lembre-se de que algumas informações foram divulgadas pouco depois da Tempestade no Deserto, revelando um certo grau de interferência, por parte dos Estados Unidos, nas comunicações do Iraque, e outras atividades. Acho que podemos dizer que talvez esse tenha sido o primeiro exemplo do uso da guerra de informação. Na verdade, isso não é novidade. Há anos, e até mesmo décadas, estamos tentando desestruturar as comunicações do inimigo e descobrir os seus códigos, etc. — tudo isso faz parte da mesma coisa. Só que agora temos uma versão muito mais sofisticada dessa atividade.

P: O que o senhor está planejando na subcomissão, no momento, no que se refere a outra atividades?

KYL: A próxima coisa que faremos é rever o relatório que será emitido em novembro em resposta à Determinação Presidencial (PDD), que nos dará alguma indicação dos rumos que o governo pretende tomar, avaliar essas informações, talvez convocar uma audiência para saber o que eles pretendem fazer e talvez consultar outras pessoas que podem ter opiniões diferentes, e, não sei, na atual conjuntura, o que faremos depois disso.

P: O senhor acha que grandes dotações orçamentárias serão necessárias em algum momento?

KYL: Os valores são relativamente pequenos, na verdade, mas eu diria que haverá necessidade de algumas verbas.

FANTASMAS NAS MÁQUINAS?

Dr. Martin Libicki

Analista Político Sênior, RAND

O autor cita a execução da lei como uma das principais áreas nas quais a segurança global de informação pode ser fortalecida. Ele pede "a harmonização das leis nacionais contra os ataques aos computadores, a cooperação multinacional quando se tratar de rastrear ataques de um país para outro, acordos internacionais para a extradição das pessoas responsáveis pelos ataques, e disposição para impor sanções às pessoas que protegerem os autores dos ataques." Ele acredita que a boa vontade para compartilhar informações sobre pesquisa e desenvolvimento, sobre indicações e advertências de ataques, e sobre a ocorrência e a reação a ataques "também pode reforçar a eficácia das medidas de proteção de cada nação."

Quem estiver procurando novos motivos para preocupação não precisa ir muito longe. Em todos os lugares, os computadores e outros aparelhos digitais entraram nas nossas vidas. O que era manual, agora é automático; o que era analógico, agora é digital; e o que, no passado, funcionava isoladamente, agora está ligado a todas as outras coisas. A cada dia que passa, não temos escolha: temos que contar com essas máquinas. Se elas falharem, naufragaremos.

A fé resultante da dependência seria merecida se esses dispositivos somente fizessem o que devem. Alguns falham por conta própria, e nós seguimos em frente. Mas também existe a possibilidade de eles falharem por terem caído nas mãos daqueles que querem agir de modo a nos prejudicar. Em tais circunstâncias, eles podem não apenas deixar de funcionar, mas podem também revelar segredos a eles confiados, ou produzir informações corrompidas — às vezes de tal forma que o fato só pode ser percebido quando já é tarde demais para reverter as ações que já se encontram em andamento.

Por que existe essa vulnerabilidade? Os equipamentos digitais são rápidos, baratos, precisos, e raramente esquecem o que dizemos a eles. Mas eles são absurdamente literais e geralmente não possuem o discernimento para compreender as implicações das ordens que recebem e nem a integridade das pessoas que dão essas ordens.

As conseqüências em potencial de falhas ou corrupção de sistemas, deliberadamente induzidas, são enormes. Assumindo o controle dos principais sistemas que dão suporte à sociedade, os atacantes da informática podem, em teoria, escutar ligações telefônicas, fazer ligações para os lugares errados, e tornar os serviços de telefonia totalmente inoperantes; interromper o fornecimento de energia elétrica; interferir na realização de negócios da ordem de, literalmente, trilhões de dólares por semana; prejudicar os serviços de emergência; impedir as forças armadas dos Estados Unidos de reagir a crises no exterior rapidamente; revelar informações médicas de caráter pessoal e secreto; criar confusão nos sistemas de transporte, e criar situações de perigo para os viajantes; e muito mais. A vida, como a conhecemos, poderia ficar paralisada.

Os ataques a computadores, se forem suficientemente sistemáticos, podem ser uma guerra por outros meios — essa é a origem do termo "guerra de informação" como um conceito abrangente. Mas a guerra de informação no sentido mais amplo — atacar as informações e o processo de tomada de decisões de um adversário — é tão antiga quanto a guerra propriamente dita. Tais táticas abrangem operações psicológicas, ataques à estrutura de comando de um inimigo, espionagem e contra-espionagem, e operações contra as infra-estruturas e os sistemas de vigilância do adversário. Durante a Guerra Civil dos Estados Unidos (1861-1865) houve incidentes de operações de propaganda, atiradores de elite alvejando generais inimigos e observadores em balões de ar quente, sabotadores destruindo linhas telegráficas, piquetes de cavalaria e manifestações contra a cavalaria — todas essas coisas constituem guerra de informação. Na

Segunda Guerra Mundial surgiu a guerra eletrônica sob a forma de radar, despistamento eletrônico, bloqueio de radiofreqüência, elaboração de códigos, e a decifração de códigos auxiliada por computador.

Os ataques a computadores se encaixam muito bem nesse tipo de guerra. Se é possível destruir o quartel-general do inimigo com bombas e tiros, o que há de errado em utilizar meios menos violentos de invadir e neutralizar os sistemas de computação que gerenciam as batalhas do futuro? Em 1920, havia noções de guerra estratégica segundo as quais o uso da força aérea contra alvos civis reduziria ou talvez evitaria a carnificina da guerra de trincheiras. A guerra estratégica pela informação vai um passo além disso.

As sociedades modernas são vulneráveis? A maioria dos sistemas de informação tem muito menos segurança do que poderiam; muitos têm menos do que deveriam ter. Redes e sistemas de muitos tipos já foram atacados — o serviço da Internet, o serviço de telefonia, alguns serviços de transporte, instituições financeiras, e redes corporativas.

Os ataques a computadores são, de qualquer maneira, um problema sério. Na verdade, o Federal Bureau of Investigation [FBI — polícia federal americana] recentemente estimou que eles têm um custo, para a economia americana, que varia entre meio bilhão e cinco bilhões de dólares por ano — uma estimativa com uma ampla, e de certa forma, muito reveladora, margem de erro. Ninguém sabe, realmente, quantos ataques acontecem. Muitas provas são baseadas em relatos verbais, e portanto as pessoas têm que extrapolar usando conceitos populares como "somente os amadores deixam impressões digitais, os profissionais nunca o fazem", e, "as pessoas nunca querem dizer com que gravidade foram atingidas." Portanto, os ataques a computadores são comparados aos icebergs, e o país, supostamente, faz o papel do Titanic.

De qualquer maneira, esta é a teoria. Mas essa teoria é uma perspectiva? Ao contrário de todas as outras formas de guerra, não se entra no espaço cibernético à força. Se os hackers penetram em um sistema, eles invariavelmente o fazem usando caminhos residentes no próprio sistema: alguns são características e alguns são "bugs" (isto é, características não documentadas), que nunca são removidos. De qualquer forma, o deslocamento ao longo desses caminhos está totalmente sob o controle de quem quer que esteja operando o sistema. Assim, a vigilância é tudo o que é necessário para a proteção.

De fato, existem proteções. Muitos sistemas de informação operam em vários níveis: há maneiras de estabelecer uma distinção entre os usuários legítimos e os ilegítimos, barreiras para impedir que os usuários legítimos assumam o controle dos sistemas de computação, intencionalmente ou não, e dispositivos de segurança, para que nem mesmo a usurpação do controle crie um perigo para o público.

Os atacantes, por sua vez, precisam, antes de mais nada, enganar o sistema, fazendo com que ele acredite que eles são usuários legítimos (por exemplo, roubando ou adivinhando uma senha) e em seguida, adquirir privilégios de controle (freqüentemente explorando falhas endêmicas) que são negados à maioria dos usuários comuns. Com esses privilégios de "super-usuários", os atacantes podem eliminar arquivos-chave, escrever coisas sem nexo em outros, ou instalar uma "porta dos fundos" para poderem entrar novamente mais tarde.

Ninguém duvida de que as defesas, se necessário, podem ser melhores do que a prática comum atual.

A maioria dos sistemas usa senhas para limitar a entrada, mas as senhas apresentam muitos problemas que são bem conhecidos: muitas delas podem ser facilmente adivinhadas; elas podem ser roubadas ao fluírem pelas redes, e além disso, elas freqüentemente ficam armazenadas em partes do servidor onde se espera que elas possam ser encontradas. Os métodos de encriptação como assinaturas digitais contornam esses problemas (a captura e a reprodução de mensagens de acesso não funciona) . As assinaturas digitais até ajudam a garantir que qualquer mudança em um banco de dados ou programa, uma vez assinada eletronicamente, pode ser usada para localizar o seu autor — o que também é útil, se o atacante for alguém que pertence à organização e que possua privilégios para utilizar os sistemas.

Os sistemas operacionais de computadores e redes são vulneráveis a programas inseridos pelos hackers, como vírus (software que infecta software e faz com que ele

infecte outro sofware), cavalos de Tróia (Trojan horses) (software aparentemente útil, que contém armadilhas ocultas) e bombas de lógica (software que fica latente até ser acionado por um sinal). Os programas de proteção contra vírus podem funcionar, mas se as preocupações persistirem, por que não colocar todos os arquivos críticos em uma mídia que não possa ser alterada (por exemplo, um CD-ROM)? Uma mídia desse tipo pode, também, impedir que informações sejam apagadas ou corrompidas pelas pegadas digitais de um atacante em potencial. Na verdade, devido ao baixo custo de tais dispositivos, já não existe mais uma desculpa legítima para perder informações.

Os sistemas podem também ser colocados em uma situação de risco por causa de outros sistemas que são considerados confiáveis. Duas precauções podem ser tomadas contra esse perigo: reduzir a lista de sistemas confiáveis e limitar o número de mensagens às quais um determinado sistema reage. Nos sistemas bancários, por exemplo, isso é feito para impedir que os computadores sejam corrompidos por caixas automáticas localizadas em alguma esquina. O computador ignora qualquer coisa oriunda de uma caixa automática que não seja uma transação legítima. Nenhuma transação legítima pode causar danos ao computador do banco.

Uma última precaução é puxar a tomada. Em casos extremos, muitos sistemas (por exemplo, as usinas atômicas) funcionam quase perfeitamente se forem desconectadas do resto do mundo.

Até que ponto os proprietários de um sistema devem ir? Uma proteção de baixo custo (por exemplo, paredes de fogo [firewalls] e detectores de invasão) podem parecer o suficiente para o ambiente atual. Afinal, talvez não valha a pena gastar uma quantia muito alta para proteger o sistema de um escritório se, por exemplo, um ataque somente causará uma interrupção temporária no seu funcionamento. Muitas empresas não consideram a ameaça séria e investem proporcionalmente. Elas podem estar certas. Mas e se elas estiverem erradas? Se e quando as ameaças crescerem, os proprietários dos sistemas podem elevar o nível de segurança — até mesmo a curto prazo (por exemplo, impedindo que os usuários se conectem de suas casas ou que executem certas ações quando estiverem conectados).

Na verdade, é justamente a falta de boas características de segurança em toda a infra-estrutura nacional de informação, na atualidade, que dá margem a uma certa confiança de que os sistemas de computação poderiam, se necessário, se tornar seguros. (Em comparação, boas defesas contra a guerra nuclear foram tecnicamente impossíveis de conseguir durante décadas, e se possíveis hoje, têm um custo muito elevado.) Mesmo se muitos sistemas puderem ser neutralizados temporariamente, mantê-los fora do ar por muito tempo já não será tão fácil, enquanto os administradores dos sistemas estiverem trabalhando freneticamente para fazer com que os serviços essenciais voltem a funcionar. Qualquer um que queira colocar a infra-estrutura de informação dos Estados Unidos em uma situação de risco deve compreender que a simples ameaça de fazer isso — se for levada a sério — será neutralizada pouco tempo depois de ser anunciada, à medida que as pessoas reagirem.

Qual deve ser o papel do governo? As pessoas responsáveis pela proteção da nação em terra, na água e no ar, e no espaço exterior também podem proteger a nação no espaço cibernético? Será que elas devem fazer isso?

O governo pode ajudar, mas há muita coisa que o governo não pode fazer — ou não deve fazer. Sim, a eletricidade é essencial, mas a proteção do fornecimento da energia elétrica contra a ação dos hackers depende quase inteiramente da maneira pela qual as empresas de energia administram os seus sistemas de computação: isso inclui o software de rede e o sistema operacional que elas compram, a maneira pela qual esse software é configurado, como os privilégios de acesso são atribuídos e protegidos, e como os vários mecanismos à prova de falha e de sobrepujamento manual estão instalados nos sistemas de geração e distribuição da empresas. É inadmissível que qualquer empresa de energia queira que o governo a "proteja" dizendo-lhe como fazer essas coisas. Em termos mais gerais, o governo não pode construir uma parede de proteção em torno dos Estados Unidos — até porque muitas redes internas se estendem pelo mundo inteiro.

O governo pode fazer cumprir leis contra ataques a computadores, e faz isso. Ele tem sido muito bem sucedido, levando-se em consideração que os atacantes podem ser tão anônimos e tão distantes. Até agora, a

maioria dos ataques de hackers mais comentados foram executados não por profissionais, mas por amadores.

O governo deve tentar inibir a guerra de informação ameaçando se vingar dos culpados? Vamos assumir que eles possam ser identificados. O governo dos Estados Unidos pode ameaçar agir da mesma forma, mas muitas nações não confiáveis têm poucos sistemas comparáveis aos nossos (por exemplo, a Coréia do Norte não tem uma bolsa de valores para ser neutralizada). Por outro lado, é problemático reagir violentamente a um ataque de guerra de informação que tenha causado perdas à vítima, em termos de tempo e dinheiro, mas que não tenha ferido ninguém.

Embora muitas coisas que o governo pode fazer para fortalecer a segurança sejam indiretas, a Comissão Presidencial Sobre a Proteção à Infra-Estrutura Crítica, e outras entidades, fizeram as seguintes recomendações:

— Certifique-se de que os próprios sistemas do governo estejam protegidos, porque eles são importantes para a segurança nacional e para estabelecer um padrão para outras organizações.

— Utilize pesquisa, desenvolvimento, e aquisição de primeiro usuário para promover o desenvolvimento rápido das ferramentas de segurança.

— Divulgue avisos sobre ataques iminentes relacionados à guerra de informação (se eles puderem ser detectados — essa não é uma tarefa fácil).

— Promova uma estrutura legal que induza os usuários privados a proteger os seus sistemas o máximo possível dentro das suas possibilidades.

— Promova um ambiente neutro de coleta, seleção e distribuição de informações que estimule os usuários privados para que eles compartilhem as suas experiências e contramedidas, confidencialmente.

De modo geral, essas medidas estão sendo implementadas. ◉

A REAÇÃO DO ENSINO SUPERIOR À GUERRA DA INFORMAÇÃO

Dr. Charles W. Reynolds
Diretor do Departamento de Ciência da Computação e Reitor Interino
Faculdade Integrada de Ciência e Tecnologia [College of Integrated Science and Technology]
Universidade James Madison

Há uma procura cada vez maior por profissionais de segurança de informação em uma era em que toda uma série de atividades, como "o vandalismo mal-intencionado, a atividade criminosa, e a guerra de informação em nível internacional" pode ameaçar a infra-estrutura de informação do país, diz o Dr. Charles Reynolds. Ele descreve a maneira pela qual a comunidade acadêmica está colaborando com o governo e com a comunidade empresarial para preencher esse requisito, por meio de uma iniciativa, que surgiu em 1997, chamada Colóquio Nacional Para a Educação em Segurança de Sistemas de Informação [National Colloquium for Information Systems Security Education] (NCISSE). O autor, que é presidente, para o ano de 1998, do comitê executivo do NCISSE, também descreve os esforços da Universidade James Madison para atender às prioridades nacionais que estão surgindo, no sentido de reagir às ameaças às redes de informação dos Estados Unidos.

A NECESSIDADE DE PROTEÇÃO DA INFRA-ESTRUTURA DE INFORMAÇÃO E COMUNICAÇÃO

Todos os aspectos das nossas vidas e todos os aspectos dos nossos sistemas social, político e econômico estão se tornando cada vez mais dependentes da nossa infra-estrutura de informação e comunicações. Os nossos sistemas financeiros, os nossos sistemas de transporte, as nossas empresas de fornecimento de água e energia elétrica, e todas as outras infra-estruturas críticas se tornaram dependentes da nossa infra-estrutura de informação e comunicações. No entanto, essa infra-estrutura é a mais vulnerável de todas as nossas infra-estruturas no que diz respeito ao vandalismo mal-intencionado, à atividade criminosa, e à guerra de informação em nível internacional — todas essas coisas podem ameaçá-la e portanto, ameaçar todas as outras infra-estruturas que dela dependem. A segurança e a garantia da nossa infra-estrutura de informação e comunicações, portanto, são prioridades nacionais.

Para enfrentar as ameaças da nova era da tecnologia de informação, a nossa nação precisa de um contingente de trabalhadores familiarizados com informática, que estejam cientes das vulnerabilidades que estão surgindo nas infra-estruturas críticas, assim como um quadro de profissionais de segurança em informação que conheçam as "melhores práticas" reconhecidas na área da segurança de informação e da garantia da informação.

UM DIÁLOGO NACIONAL COM O ENSINO SUPERIOR

Em resposta à necessidade de proteger as infra-estruturas críticas da nação, o Colóquio Nacional Para a Educação em Segurança de Sistemas de Informação [National Colloquium for Information Systems Security Education] (NCISSE) foi criado em maio de 1997, para proporcionar um ambiente para o diálogo entre as lideranças no governo, no meio empresarial e no meio acadêmico, sobre as maneiras de se trabalhar em parceria para definir os requisitos atuais e os que estão surgindo, no que diz respeito à educação na área de segurança da informação. O NCISSE também procura influenciar e estimular o desenvolvimento e a expansão de currículos de segurança da informação, especialmente nos níveis de graduação e pós-graduação.

Na sua segunda reunião anual em junho de 1998, na Universidade James Madison em Harrisonburg, Virginia, o Colóquio concordou com a missão do NCISSE de tentar estimular o desenvolvimento de currículos acadêmicos que reconheçam as necessidades expressas pelo governo e pela comunidade empresarial, e que sejam baseados nas "melhores práticas"

reconhecidas, que estiverem disponíveis no campo.

Os objetivos do Colóquio também se concentram na necessidade de auxiliar as instituições de ensino, apoiando o contínuo desenvolvimento e a partilha de recursos de educação em segurança de informação. O NCISSE estimula as instituições de ensino para que elas promovam cursos adequados de segurança de sistemas de informação em vários currículos, para atender às necessidades dos clientes do século XXI; há também um estímulo para que sejam oferecidos cursos para atender à demanda crescente de profissionais na área de segurança de sistemas de informação.

Na sua reunião anual de 1998, o NCISSE divulgou uma agenda abrangente que previa ações dos seus vários componentes. Essas ações incluíam tarefas para o governo, empresas, e instituições de ensino superior, que deveriam ser executadas tanto individualmente quanto sob a forma de cooperação entre os setores.

Um item particularmente importante entre as ações conjuntas que se fazem necessárias é a determinação precisa do conhecimento, habilidades, e atitudes que definem um profissional de segurança em informação, e portanto, o desenvolvimento de normas sobre o que os profissionais de segurança de informação devem saber e o que devem ser capazes de fazer. Como a segurança de informação propriamente dita ainda se encontra em fase de formação como ramo do conhecimento, precisamos identificar as "melhores práticas" atuais, para inclusão nas normas profissionais de maneira que a evolução possa ser contínua. Finalmente, todos os três componentes do Colóquio devem vencer a resistência do pessoal de segurança de informação em relação às normas, porque a observância da disciplina incorporada às normas é o que se espera de qualquer profissão.

Descrevendo também as ações recomendadas para as empresas privadas, o Colóquio afirmou que o setor empresarial deve proporcionar, às instituições de ensino, verbas, equipamentos, e software, e deve ajudar na manutenção dos sistemas de computação nos campi das universidades; deve, ainda, proporcionar treinamento no local para os professores das universidades, incluindo aqueles que não tenham trabalhado anteriormente com segurança de informação; e deve patrocinar estágios para que os alunos possam trabalhar na área de segurança de informação.

O NCISSE insistiu para que o governo desenvolvesse e compartilhasse materiais para cursos na área de segurança de informação, e que encorajasse o desenvolvimento de Centros Para a Proteção da Infra-Estrutura, nas universidades, utilizando, como modelo, os Centros de Materiais patrocinados pela Fundação Nacional da Ciência [National Science Foundation] e os Centros de Transportes, patrocinados pelo Departamento dos Transportes [Department of Transportation].

Os membros do Colóquio também pediram aos profissionais de segurança de informação no país inteiro que melhorassem a rede de relações entre os membros do corpo docente, patrocinassem mais conferências sobre segurança de informação, criassem mais sites na Web, e publicassem mais revistas especializadas sobre a proteção das redes de informação dos Estados Unidos. Eles também reafirmaram a necessidade de estabelecer um sistema formal de reconhecimento dos programas de educação sobre segurança de informação que se destacassem.

Com um enfoque nas instituições de ensino superior, o NCISSE estimulou as instituições de ensino no sentido de aumentar o número de programas com ênfase em segurança de informação, e incluir cursos de segurança nos currículos básicos de todas as pessoas que se formarem nas universidades.

Uma coisa particularmente importante é a inclusão de currículos que tratem das questões éticas e culturais que surgem nos sistemas modernos de informação. As questões, nessa área, incluem a maneira pela qual os valores tradicionais são preservados na era da informação moderna e como eles podem requerer mudanças.

Como muitos valores éticos e culturais são formados nos primeiros anos de vida, as instituições de ensino superior são encorajadas no sentido de desenvolver currículos de segurança de informação para a educação secundária e em colaboração com ela.

Em sinal de reconhecimento de que o ensino superior, pelos seus próprios méritos, é uma profissão que segue normas, as instituições de ensino foram estimuladas a

solicitar orientação de organizações de credenciamento para a incorporação, de forma apropriada, da segurança de informação nos seus currículos.

Finalmente, como a educação é uma questão que dura a vida inteira em uma sociedade tecnológica que evolui rapidamente, o ensino superior foi estimulado no sentido de proporcionar programas de aperfeiçoamento para os profissionais de segurança de informação que já estiverem trabalhando no campo.

O Colóquio recomendou que os educadores da área de segurança de informação desenvolvessem e compartilhassem exercícios práticos de laboratório sobre a segurança de informação, projetassem jogos para computadores que expressassem valores apropriados para um quadro de profissionais responsáveis e familiarizados com informática, desenvolvessem um lugar para compartilhar material de ensino, e escrevessem mais livros-texto, particularmente a respeito de questões práticas.

A agenda do NCESSE para providências também pedia que os especialistas no ensino da advocacia ajudassem os advogados dos Estados Unidos a entender a segurança de informação.

MÉTODOS DE ENSINO BASEADOS NA INTERNET

A crítica necessidade de profissionais de segurança de informação é uma coisa típica do mundo moderno, em que a tecnologia impera. Como a tecnologia muda rapidamente, os profissionais devem ter um compromisso de aprendizado para o resto da vida, que constantemente renove e amplie as suas habilidades. E todos os profissionais devem estar preparados para reorientar suas carreiras e adquirir novas habilidades, pois a tecnologia, que está sempre passando por mudanças, determina as necessidades, sempre em mudança, da força de trabalho.

A necessidade de profissionais de segurança de informação se multiplicou nos últimos anos. Essa necessidade de profissionais especializados, por sua vez, criou a necessidade de oportunidades de educação que formem novos profissionais e que reorientem os atuais profissionais em uma nova direção. No entanto, não se deve esperar que esses profissionais que estão à procura de cursos de especialização interrompam as suas atuais carreiras e vidas em família para freqüentar uma universidade tradicional em um campus. É por isso — devido à necessidade de cursos de especialização para profissionais adultos que não interrompam suas carreiras ou vidas em família — que existe tanto interesse na educação baseada na Internet. A Universidade James Madison reagiu a essa necessidade e à tecnologia da Internet com um programa profissional em nível de pós-graduação, sobre a segurança da informação, baseado na Internet.

O currículo é oferecido sob a forma de um programa de aprendizado baseado na Internet, por meio e contratos com organizações que possam garantir a integridade dos procedimentos de testes para os seus empregados.

O programa é estruturado sob a forma de 13 cursos de sete semanas cada um, e a sua duração é de pouco mais de dois anos. Um grupo de alunos inicia o programa na mesma data. O grupo continua junto e completa todos os 13 cursos em seqüência. O grupo é chamado de "cohort" (turma) pela universidade.

O programa de aprendizado baseado na Internet combina o estudo independente com a instrução orientada e a colaboração entre os membros de um grupo. As atividades são coordenadas por uma central que proporciona uma rede de serviços. Os professores e a tecnologia proporcionam um sistema de entrega que mantém altos padrões acadêmicos, e ao mesmo tempo é flexível e leva em consideração as necessidades dos participantes. Grupos de discussão — por meios eletrônicos — examinam, discutem, e fazem uma análise crítica de conceitos de segurança de informação. Cada curso consiste em uma sequência de leituras e problemas que devem ser resolvidos.

As apresentações, na Internet, de conceitos, podem ser vistas em qualquer estação de trabalho conectada à Internet, em qualquer lugar do mundo a qualquer momento. Os projetos em cada classe oferecem orientação prática em relação aos conceitos e materiais que são estudados.

O PROGRAMA DE SEGURANÇA DE INFORMAÇÃO NA UNIVERSIDADE JAMES MADISON

Os participantes que completam o Programa de Segurança de Informação na Universidade James Madison recebem o título de mestrado em ciência da computação, com ênfase em segurança da informação. O programa é baseado em um padrão endossado pela Agência Nacional de Segurança [National Security Agency] e tem como objetivo desenvolver os conhecimentos e as habilidades necessários para que se compreenda as inter-relações entre a segurança da informação e a tecnologia da informação, e para relacionar os componentes técnicos e humanos da segurança de informação e da tecnologia de informação.

A base dos cursos conduzidos pelos professores da Universidade James Madison enfatiza a administração, gerenciamento, avaliação e implementação da tecnologia de computação com ênfase na segurança da informação. O gerenciamento dos programas de segurança de informação inclui a preservação e a proteção da confidencialidade, integridade, disponibilidade, autenticidade e utilidade das informações, dentro dos limites aceitáveis de risco.

Os membros do programa, trabalhando em equipe:

— Desenvolvem o conhecimento e as habilidades necessários para que se possa compreender a relação entre a segurança de informação e o avanço das tecnologias de sistemas de informação necessários para implementar programas de proteção contra crimes e detecção dos mesmos;

— Desenvolvem competências avançadas relacionadas a posições nas áreas técnicas, de supervisão, de política, e outras, nas áreas de segurança de informação e tecnologia da computação, no que se refere à avaliação de vulnerabilidades, ameaças e riscos;

— Adquirem as perspectivas necessárias, de analistas eficazes de segurança de informação, gerentes, administradores, e praticantes no que se refere ao planejamento, avaliação, e implementação de técnicas e programas de segurança de informação;

— Relacionam os componentes técnicos e humanos da segurança de informação e da tecnologia da computação na proteção dos sistemas de informação;

— Desenvolvem as competências básicas em projeto de bancos de dados e sistemas de informação, na operação de sistemas e redes, e na aplicação de desenvolvimentos de software para aperfeiçoar as atribuições de prevenção do crime e de investigação.

O programa tem início com um segmento preparatório para as pessoas que precisam reforçar suas habilidades da área da computação antes de entrar na parte de ciência da computação. Essa fase é seguida de três cursos de ciência da computação que cobrem o gerenciamento de bancos de dados, a operação de sistemas e redes, e o desenvolvimento de programas aplicativos. A partir dessa base sólida, o terceiro período apresenta a segurança de informação, os conceitos dos sistemas de informação dos quais se confia, e técnicas para o armazenamento e a transmissão de informações protegidas, especialmente por meio de criptografia. O quarto segmento apresenta questões de gerenciamento e administração no que se refere à segurança de informação, incluindo análise de risco e vulnerabilidade, ferramentas e procedimentos de auditoria de sistemas de informação, e questões legais, éticas e de política. Um projeto de final de curso integra o programa na sua totalidade com um projeto que desafia os participantes a analisar a segurança de um sistema de informações.

O CURRÍCULO DE SEGURANÇA DE INFORMAÇÃO NA UNIVERSIDADE JAMES MADISON

O programa de segurança de informação da Universidade James Madison inclui os seguintes cursos organizados em segmentos:

1. Segmento Básico de Ciência da Computação

Sistemas Operacionais e Redes — Conceitos e princípios de sistemas operacionais de múltiplos usuários. Memória, CPU (unidade central de processamento), atribuição de dispositivos de I/O (entrada e saída), e segurança. Hierarquias de memória, avaliação de desempenho, modelos analíticos, simulação, programação simultânea, e processadores paralelos.

Sistemas de Gerenciamento de Bancos de Dados — Tipos de armazenamento físico e métodos de acesso; modelos de dados; álgebra racional e cálculo, e linguagens de definição e busca; dependências, decomposição e normalização, projeto de bancos de dados; recuperação; consistência e simultaneidade; bancos de dados distribuídos. Exemplos de bancos de dados comerciais.

Desenvolvimento de Programas Aplicativos — O ciclo de vida do desenvolvimento de software, gerenciamento de projetos de software, ferramentas e métodos de desenvolvimento, garantia da qualidade de software, paradigmas de linguagens de programação e sua utilização em desenvolvimento de software.

2. O Segmento Técnico da Segurança de Informação

Introdução à Segurança de Informação — Visão geral das ameaças à segurança dos sistemas de informação, responsabilidades e ferramentas básicas para a segurança da informação, e para as áreas de treinamento, e a ênfase necessária em organizações para obter e manter uma situação de segurança aceitável.

Sistemas nos Quais se Confia — Definição de um "Sistema no Qual se Confia" e considerações a respeito do projeto, avaliação, certificação e credenciamento de sistemas confiáveis, incluindo considerações sobre hardware, considerações sobre software, como controles de desenvolvimento, validação/verificação, distribuição garantida e outras questões de garantia. Implementação, gerenciamento de configuração, e administração de sistemas confiáveis. A importância de se compreender a psicologia e o modo de vida bem sucedido do atacante, para gerar e manter uma defesa poderosa.

Criptografia — Este curso proporciona ao aluno uma compreensão e a capacidade de implementar os principais protocolos de criptografia. Ele lida com o projeto e a análise que proporcionam proteção para as comunicações ou que resistem à análise criptográfica.

3. Segmento de Gerenciamento de Segurança de Informação

Vulnerabilidade, Risco, e Análise de Sistemas de Informação — As vulnerabilidades e os riscos inerentes à operação e à administração de sistemas de informação são identificadas e exploradas.

Controles de Auditoria de Segurança de Informação — Os alunos desenvolvem planos e conduzem uma auditoria de segurança de informação, incluindo uma pesquisa de segurança em profundidade. Eles desenvolvem e implementam padrões para a monitoração das atividades normais de um sistema de informação

Política, Procedimentos, Questões Legais e Ética — Desenvolvimento, avaliação, e implementação de políticas e procedimentos de segurança administrativa em um sistema UNIX, em um ambiente seguro. Preparação de um Guia de Segurança Administrativa ou de um anexo para um documento desse tipo.

4. Projeto Final de Segurança de Informação

Um projeto final integra o programa na sua totalidade, com um projeto que lança um desafio para que os participantes analisem a segurança de um sistema de informação, estudem e analisem a eficácia das opções disponíveis para reforçar essa segurança, analisem o contexto legal e ético dessas opções, sob um ponto de vista mais amplo, e selecionem e proponham um procedimento de implementação para uma da opções.

Aulas Preparatórias — Os alunos que não se encontrarem em condições de iniciar os segmentos básicos podem se matricular em uma seqüência preparatória de três aulas: Curso Acelerado Sobre os Fundamentos de Programação de Computadores, Fundamentos Avançados de Programação de Computadores, e um Curso Acelerado Sobre os Fundamentos dos Sistemas de Computação.

OS SETORES PÚBLICO E PRIVADO SE BENEFICIAM, COMPARTILHANDO CONHECIMENTOS E TÉCNICAS DE SEGURANÇA

Uma entrevista com Howard Schmidt

Diretor de Segurança de Informação, Microsoft Corporation

Os órgãos do governo e muitas empresas privadas agora têm a possibilidade de "se contatar e se apoiar mutuamente", no caso de surgirem ameaças contra os seus sistemas de informação ou outros sistemas críticos, diz Howard Schmidt, Diretor de Segurança de Informação da Microsoft Corporation. Ele também menciona o fato de que há muita cooperação entre as empresas quando se trata de lidar com questões referentes à guerra de informação. "Quando se trata de questões de segurança, há muito poucas coisas relacionadas à concorrência." Schmidt diz. "Trabalhamos com os nossos concorrentes, e também com os nossos parceiros, para ajudar a desenvolver padrões para que todos nós sejamos bem sucedidos no desenvolvimento e na manutenção de um bom nível de segurança." Schmidt foi entrevistado pelo Editor Executivo Dian McDonald.

Pergunta: Como o senhor avalia a vulnerabilidade das infra-estruturas críticas dos Estados Unidos aos ataques cibernéticos? Até que ponto os Estados Unidos estão preparados para suportar tais ataques?

Schmidt: A minha avaliação é a mesma da Comissão Presidencial Sobre a Proteção da Infra-Estrutura Crítica: Temos algum trabalho a ser feito. Essas eram questões, que quando a comissão estava sendo estabelecida, não estavam, realmente, em primeiro plano. No que diz respeito à nossa capacidade de suportar tais ataques, eu acho que a Comissão Presidencial Sobre a Proteção da Infra-Estrutura Crítica já percorreu um longo caminho no seu trabalho de unir os setores privado e público para poder resistir, em conjunto, a esses tipos de ataques, e basicamente, fazer um ótimo trabalho quando se tratar de reagir a eles.

P: O senhor trabalhou com a comissão?

Schmidt: Sim, já trabalhamos com a comissão. Eles estiveram aqui (em Redmond, Washington) para algumas reuniões. E eu fui a Washington, D.C. para participar de algumas reuniões. E, na verdade, estamos montando uma equipe bem grande de pessoas do governo e do setor privado. Estamos unindo essas pessoas para que possamos chegar a um acordo sobre as maneiras de termos uma infra-estrutura melhor.

P: Que mudanças organizacionais a sua empresa fez como resultado das novas ameaças à tecnologia?

Schmidt: Permita-me reformular a pergunta, porque nós não consideramos essas coisas ameaças à tecnologia. O que estamos vendo é o uso da tecnologia para dar a alguém uma oportunidade de ir em frente e fazer alguma coisa contra um público-alvo maior, por assim dizer. Basicamente, o que estamos vendo é isto: os mesmos velhos tipos de ameaça continuam por aí, mas agora eles estão usando a tecnologia mais nova.
Para reagir a isso, criamos, um ano atrás, um programa do qual estamos muito orgulhosos: o MIAP, ou Microsoft Information Assurance Program (Programa de Garantia da Informação, da Microsoft), que nos dá condições de unir muitos dos interesses, internamente, que seriam relativos à proteção da nossa informação, ao ato de garantir que a nossa informação é válida. Agora temos, sob um "guarda-chuva" organizacional, vários programas e funções, incluindo o nosso plano de recuperação para casos de desastres, o nosso sistema de retenção e classificação de dados, a nossa estratégia de reserva, o grupo de segurança de informação propriamente dito, o grupo de segurança física, na medida em que ele se relaciona com a garantia da informação, assim como o grupo de segurança de produtos, pois a Microsoft é uma empresa de desenvolvimento de software.
Sob essa estrutura, temos a alimentação cruzada e a utilização cruzada de todas as especialidades, não apenas para proteger as nossas informações e sistemas, mas para assegurar que os produtos nos quais estamos trabalhando no momento se beneficiem da experiência da pessoas que estão no campo de segurança de

informação, para ajudar a aperfeiçoá-los.

P: Em termos de estratégias para lidar com a guerra de informação, até que ponto o senhor está trabalhando em conjunto com outras empresas?

Schmidt: Estamos trabalhando muito. Para dizer a verdade, temos vários grupos diferentes: por exemplo, a Associação Para a Segurança de Sistemas de Informação [Information Systems Security Association], que é uma entidade sem fins lucrativos cujos membros estão envolvidos com o campo de segurança – por exemplo, representantes da Charles Schwab Company, da U.S. Space Alliance, da Air Touch Cellular, e vários órgãos governamentais. Participamos de conferências, e trabalhamos com o Gartner Group, uma grande empresa de consultoria na área de computação. Fazemos parte da iniciativa do ex-senador Sam Nunn, que tem colaborado muito na área de proteção de infra-estrutura. Ele coordena um grupo de discussão sobre segurança que se reúne periodicamente no Instituto de Tecnologia da Georgia [Georgia Institute of Technology], em Atlanta, e temos participado desse grupo também.

Portanto, há muito intercâmbio de informações e de "melhores práticas" entre nós, no campo da segurança, no setor privado. E há outros grupos, como o Comitê Federal de Investigações na Área da Computação [Federal Computer Investigations Committee] e a Associação de Investigadores de Crimes de Alta Tecnologia [High Tech Crimes Investigators' Association], que são formados por representantes tanto do setor público quanto privado que trabalham em conjunto nessa área. Portanto, temos algumas relações muito boas, e trabalhamos em estreita colaboração. Quando se trata de questões de segurança, há muito poucas coisas que se relacionam com a concorrência. Trabalhamos com nossos concorrentes e com nossos parceiros, da mesma forma, para ajudar a desenvolver padrões para que todos nós possamos ser bem sucedidos no desenvolvimento e na manutenção de um bom nível de segurança.

P: O senhor pode falar um pouco mais sobre como a sua organização está trabalhando com o setor governamental para fazer frente aos novos desafios aos sistemas de informação?

Schmidt: Temos vários caminhos diferentes. Naturalmente, o pessoal dos produtos, que cria os produtos que nós todos usamos, tem uma relação muito forte com os funcionários de todos os órgãos governamentais, para se certificar de que os produtos estão sendo feitos para atender às necessidades do governo quando se trata de proteger a infra-estrutura crítica.
Por outro lado, como provedores de serviços on-line, nós fazemos parte da infra-estrutura, e trabalhamos muito proximamente, por exemplo, para proporcionar assistência técnica para auxiliar os indivíduos que conduzem investigações on-line. Atualmente temos um número de ajuda "24 por 7" (24 horas por dia, 7 dias por semanas) à disposição dos órgãos de segurança, para assuntos relacionados com as investigações de pessoas que estão agindo de forma ilegal na Internet.
Além disso, temos reuniões regulares a respeito das "melhores práticas". Fazemos muitas apresentações em reuniões com órgãos do governo. Por exemplo, eu fiz o discurso principal na Universidade Nacional de Defesa [National Defense University] em Washington, D.C., alguns meses atrás. Eu compareci ao evento "Defending CyberSpace '98 Conference" em Washington, D.C., em setembro. Participamos em todos esses tipos de eventos, compartilhando nossas experiências mútuas para que as melhorias daí resultantes nos beneficiem a todos.

P: O senhor acredita que o governo deve ter um papel mais importante na proteção das infra-estruturas críticas? Caso positivo, qual poderia ser esse papel, na sua opinião?

Schmidt: Basicamente, eu acredito que o governo deve continuar trabalhando em conjunto com o setor privado. Acho que a Determinação Presidencial 63 [Presidential Decision Directive 63] (PDD 63), através da qual se criou o Escritório de Garantia da Informação Crítica [Critical Information Assurance Office], realmente proporciona uma boa estrutura para colocar o governo em uma boa posição para trabalhar com o setor privado. E eu acho que com essa função governamental – e sem nenhuma legislação nova, sem novas normas ou regulamentos – nós podemos progredir muito mais, no sentido de trabalhar com o governo para nos certificarmos de que as infra-estruturas críticas continuam, de fato, sendo um recurso protegido.

P: O senhor vê algum conflito de filosofia, nos Estados Unidos, entre os requisitos de informação no ambiente empresarial e as preocupações do governo com a segurança?

SCHMIDT: Basicamente, eu não vejo um conflito. Acho que o que nós vemos nesse aspecto é que estamos tentando nos assegurar de que temos a maior segurança, e ao mesmo tempo estamos tentando proteger a privacidade das nossas informações corporativas, informações governamentais, informações pessoais, e coisas desse tipo. Portanto, embora possa haver algumas diferenças na maneira pela qual abordamos essas questões, acho que o ponto crítico é o fato e que todos nós concordamos em uma coisa: precisamos trabalhar em cooperação, para garantir a proteção da infra-estrutura.

P: De que forma os setores público e privado podem trabalhar melhor para desenvolver capacidades eficazes de defesa contra ações terroristas ou outras ações hostis?

SCHMIDT: Acho que já falei sobre isso, mas em ultima análise, a situação é a seguinte: no momento temos, com várias agências governamentais, e muitas outras empresas, condições de nos contatarmos mutuamente e de nos apoiarmos mutuamente se algum evento desse tipo ocorrer. E eu acho que a nossa situação é muito boa quando se trata de prestar assistência técnica aos grupos de apoio dos órgãos de segurança. É claro que ainda estamos estabelecendo algumas maneiras de institucionalizar e formalizar mais esses procedimentos, mas eu acho que estamos fazendo isso agora, e vamos continuar trabalhando cada vez mais e melhor.

P: De que maneira a Microsoft incorpora segurança aos seus produtos para ajudar os clientes a se protegerem?

SCHMIDT: Isso transcende a minha área de responsabilidade, mas o que eu posso dizer é que representantes da Microsoft se reúnem periodicamente com os seus clientes. Todos nós temos preocupações com a segurança. Os empregados do departamento de desenvolvimento de produtos da Microsoft estão constantemente trabalhando para garantir que todos os produtos sejam mais seguros, e eles trabalham em conjunto conosco e com os profissionais de segurança de informação, porque aqui, nós utilizamos os nossos próprios produtos. Portanto, há um "feddback" constante, no sentido de assegurar que os produtos são tão seguros quanto possível, no momento – e também no futuro, pois mais vulnerabilidades podem ser descobertas em algum lugar.

P: O senhor acredita que com os atuais controles tecnológicos, é possível ter proteção contra vírus de computador e terroristas cibernéticos?

SCHMIDT: Recentemente tem havido muita publicidade sobre vários vírus e outras coisas que acontecem por aí. Obviamente, quando essas coisas são descobertas, trata-se apenas de mais um tipo de atividade ilícita. Nós, no setor privado e no governo, trabalhamos em conjunto para fazer frente a essas atividades e para nos certificarmos de que estaremos à frente dessas ameaças; além disso, olhamos para o futuro e tentamos prever o que alguém pode tentar fazer. Enquanto tivermos uma troca de informações e os excelentes sistemas de informação com os quais todos nós contamos, sempre haverá pessoas que tentarão fazer alguma coisa contra esses sistemas. Mas o resultado final é o seguinte: com tecnologia e educação humana e consciência dos riscos, eu acho que podemos fazer um excelente trabalho quando se trata de lidar com qualquer das questões de proteção associadas a esses recursos.

P: Os senhores desenvolveram tecnologia que poderia proteger uma empresa do envio, de forma contínua, de uma enorme quantidade de mensagens de e-mail de um terrorista cibernético?

SCHMIDT: Há uma certa quantidade de recursos embutidos, e algumas atualizações e remendos que colocamos em nossos produtos e que outras empresas colocaram nos seus produtos, para amenizar esse tipo de problema. Além disso, há algumas empresas com as quais trabalhamos no nosso Programa de Parceiros de Segurança que desenvolveram algumas ferramentas realmente muito boas – quando falo em ferramentas, estou me referindo a programas de computador – que realmente ajudariam a proteger contra ataques que se destinam a impedir o acesso a serviços, e bombas de e-mail, e coisas desse tipo. Já progredimos muito no sentido de resolver esse problema

ESTRATÉGIAS PARA FAZER FRENTE ÀS AMEAÇAS AOS RECURSOS DE INFORMÁTICA

James A. Lingerfelt
Consultor Sênior da IBM Para Questões de Segurança Pública e Justiça

A ameaça primária aos sistemas de informação não é o super-hacker maléfico, diz Lingerfelt, um perito em tecnologia e planejamento estratégico na execução da lei. "Na verdade, os maiores perigos para os sistemas de computação e os bancos de dados são as fontes 'confiáveis'". O autor ressalta que "uma avaliação realista das necessidades e ameaças em termos de segurança, seguida de uma formulação que faça sentido e da implementação de um plano de segurança, pode proporcionar proteção eficaz contra a grande maioria das ameaças, e a um custo razoável." Ele identifica as áreas que são as mais freqüentes fontes de ameaças reais e apresenta sete estratégias básicas para o planejamento da segurança na área de informática.

Os órgãos de segurança e de justiça criminal estão tendo uma oportunidade inédita de usar a informática para transformar as suas operações e para prestar um serviço melhor, mais eficaz. No entanto, muitos órgãos de segurança estão relutantes no que diz respeito a essa oportunidade, porque receiam que, substituindo ou complementando os seus sistemas mainframe, fechados, com a utilização de PCs em rede, e implementando relatórios automatizados e redes de computadores, eles se exporiam a ataques de hackers. Os altos custos estimados para se proteger todo um sistema de informática contra a penetração de super-hackers, combinados aos danos que poderiam resultar da perda de informações extremamente sensíveis, fazem com que pareça razoável evitar o risco (percebido) como um todo, apesar dos ganhos a serem obtidos com o uso da tecnologia de informação.

É verdade que devido aos aumentos exponenciais no uso da tecnologia de informação, aumenta também a exposição a ataques aos sistemas de informação, ativos, e bancos de dados. No entanto, o temido hacker de computador, dono de vastos conhecimentos de informática, raramente é a maior ameaça. Na verdade, os maiores perigos para os sistemas de computação e bancos de dados são as fontes "confiáveis" que freqüentemente operam sem receber nenhuma atenção da polícia e dos órgãos da justiça criminal no que se refere à segurança básica na área de informática. Uma avaliação realista das necessidades e ameaças à segurança, seguida de uma formulação que faça sentido e da implementação de um plano de segurança, pode proporcionar proteção eficaz contra a grande maioria das ameaças, e a um custo razoável.

PERCEPÇÃO VERSUS FATOS

Muitos departamentos têm se comprometido financeiramente, de maneira significativa, com a informática. Isso tem sido acompanhado por um aumento no número de relatos de ataques de hackers contra sistemas de informática da polícia.

Tem ocorrido, também, um aumento no número de relatos de uso ilegal de informações dos bancos de dados policiais, roubos de informações da polícia, e roubos de ativos de informática pertencentes a órgãos de segurança. A freqüência desses relatos fez com que muitas organizações policiais se sentissem desestimuladas quanto a se aventurar além dos limites dos seus sistemas existentes, fechados. No entanto, novos requisitos comerciais que recaem sobre as agências de justiça criminal exigem que elas mudem os métodos pelos quais adquirem, compartilham, e divulgam informações.

Mudanças operacionais foram iniciadas como resultado da necessidade de distribuir sistemas de informática no campo, simplificar processos de trabalho, distribuir informações além dos limites organizacionais, ou trocar informações com outros órgãos e indivíduos.

Alguns órgãos têm respondido a essas solicitações usando o seu pessoal para executar as novas tarefas, e

portanto, retirando pessoas da força disponível no campo. Outros implementaram sistemas "isolados" que somente proporcionam os novos serviços, mas não são integrados aos sistemas anteriores da organização e nem os complementam. Isso só serve para aumentar a complexidade e os custos — sob a forma de mão-de-obra, tempo e dinheiro — para se suportar os sistemas de informática.

Como já observamos, as ameaças internas de fontes de dentro do domínio no qual se confia causam mais danos do que intrusos. Vários incidentes causados por fontes internas foram documentados:

— A rede de um departamento inteiro foi nocauteada por um vírus transmitido por meio de disquetes que a divisão de planejamento do departamento distribuiu para colher informações para uma pesquisa.

— O chefe de inteligência que estava supervisionando um sistema hierárquico de inteligência fixou um bilhete no seu monitor, com uma fita, contendo a sua identidade de usuário, sua senha e instruções detalhadas para se entrar no sistema.

— Um alto funcionário de um departamento de polícia vendeu, para elementos do crime organizado, um arquivo contendo a descrição e os números das placas de todos os carros "disfarçados" usados pelos policiais.

— Um administrador de rede inexperiente, que estava instalando uma rede em um departamento de polícia, deu privilégios de administrador a todos os usuários.

— Os programadores de aplicativos em um grande departamento de polícia tiveram permissão de colocar um novo código de programa diretamente em produção, sem antes testá-lo e analisá-lo metodicamente, e o sistema ficou totalmente inoperante durante 24 horas porque o código era inadequado.

— Um governo estadual criou um site na web sem paredes de fogo. Dentro de 24 horas, a sua identificação de usuário e arquivo de senha foram colocados em uma conferência de hackers. O estado, pelo menos, fez uma coisa certa: compartilhou a sua experiência com outros estados e assim ajudou a impedir que eles cometessem o mesmo erro.

Nenhuma dessas histórias tem como personagem um super-hacker atacando o sistema de informática de um órgão do governo. O último exemplo foi uma penetração que se tornou possível pela pior porta aberta que poderia existir. Todos os incidentes poderiam ter sido evitados se tivesse havido um pouco de planejamento básico, treinamento e supervisão.

Resumindo, existe uma ameaça crescente de ataque externo como resultado do uso, cada vez mais intenso, da informática, mas a proporção da ameaça em relação ao tamanho do bolo não mudou. A única diferença é que agora o bolo é maior. Ameaça maior? Sim. Ameaça diferente? Não.

A maior exposição a ameaças à segurança na computação se deve a vários motivos:

— Novos modelos de negócios. O setor público está seguindo o exemplo do setor privado, com uns cinco anos de atraso.

— Crescimento exponencial do uso da informática: os computadores e redes se insinuaram em quase todas as áreas das nossas vidas.

— Custos reduzidos: A tecnologia atual é barata. Não importa qual seja a medida usada, os custos da informática básica estão muito mais baixos do que em qualquer época passada, e o custo das novas tecnologias está descrescendo mais rapidamente do que decrescia poucos anos atrás, por causa do rápido progresso e da maior concorrência.

NOVOS MODELOS DE NEGÓCIOS

Na transição das operações centralizadas para operações dispersas, o escritório central, como centro do universo de tomada de decisões e informações, foi substituído por unidades de negócios independentes e remotas apoiadas pela informática, que está presente em todas as unidades.

Na informática, essa mudança significou a transição das arquiteturas fechadas para as redes — intranets e extranets. A distribuição das informações significa maior

dificuldade para a proteção de ativos, para a monitoração de operações, e para a reação aos problemas. Há um número maior de pontos de exposição. A boa notícia é que a distribuição da informática está fazendo com que seja possível obter enormes ganhos em produtividade — freqüentemente o retorno do investimento ocorre em menos de um ano.

As organizações do setor privado começaram a se fixar nas competências básicas em vez de tentar proporcionar todas as coisas para todas as pessoas. As empresas estão mantendo um número de funcionários muito mais reduzido. Isso lhes permite evitar problemas trabalhistas e problemas logísticos associados às mudanças. Somente há vagas para pessoas que contribuem diretamente para o atingimento das metas do negócio. As empresas resultantes de uniões e aquisições freqüentemente apelam para a terceirização para lidar com as funções de suporte e administração, especialmente a informática. Os órgãos da justiça criminal (e o governo como um todo) começaram a avançar na mesma direção, para simplificar as operações, reduzir os custos e aperfeiçoar os serviços.

Além disso, está ficando cada vez mais difícil conservar os bons empregados da área de informática. Os governos não têm conseguido competir com os salários do setor privado para substituir os empregados que estão perdendo. Isso também tem causado um aumento no uso da terceirização na área governamental.

A maior rotatividade dos executivos e gerentes é uma realidade nas organizações, atualmente. As empresas se tornam melhores, e como elas "roubam" os empregados mais talentosos umas das outras, existe a ameaça de que os executivos ou gerentes de nível médio possam levar propriedade intelectual importante consigo. Um desse casos foi motivo de um processo bem sucedido quando se descobriu que a estrutura de diretórios dos arquivos do computador de um gerente era idêntica àquela da sua unidade de negócios anterior. Um fato raramente reconhecido ou publicado é que as empresas que reduzem o seu quadro de funcionários, freqüentemente perdem milhões de dólares devido ao roubo de hardware, software, suprimentos e mobília, quando os empregados recebem aviso prévio.

Apesar dos benefícios, a terceirização da informática pode comprometer a segurança. Um plano de segurança é particularmente importante quando responsabilidades na área de informática, que são críticas para a missão da empresa, são atribuídas a empregados contratados ou a pessoas que não pertencem ao órgão em questão. O órgão governamental pode exigir que certos requisitos de investigação de histórico pessoal sejam cumpridos por todos os empregados contratados.

CRESCIMENTO EXPONENCIAL NO USO DA INFORMÁTICA

Os computadores e as redes se insinuaram em quase todas as áreas das nossas vidas. Os computadores, redes e a Internet que todos nós usamos tornam possível a ocorrência de fraudes, roubos e disseminação de informação e materiais ilegais. Novos tipos de crimes são criados e velhas táticas ressurgem.

Felizmente esse crescimento no uso dos computadores resultou em avanços na tecnologia, normas e na identificação das melhores práticas. Todas as lições aprendidas com os erros têm contribuído para o aperfeiçoamento da tecnologia. Todos nós nos beneficiamos. As práticas de segurança também têm apresentado melhorias como resultado direto das lições aprendidas, e um sólido conjunto de melhores práticas surgiu. O setor privado preparou o terreno. A maior parte dos novos produtos (hardware e software) possui características funcionais de segurança incorporadas. Se essas características são usadas ou não é uma outra questão.

CUSTOS REDUZIDOS

Qualquer que seja o parâmetro usado, os custos da informática nunca foram tão baixos. Praticamente qualquer pessoa pode comprar um computador.

Além de a informática ter ficado mais barata, há mais dinheiro disponível para investimento em informática no setor público do que em qualquer época desde os últimos anos da década de sessenta e os primeiros da década de setenta. Por exemplo, as iniciativas relacionadas com o problema dos computadores no ano 2000 e com o crime na computação estão disponibilizando bilhões de dólares com a finalidade expressa de atualizar ou substituir os sistemas de informática do setor público. Isso cria uma oportunidade perfeita para que os órgãos de justiça criminal incluam a segurança no desenvolvimento e na

implementação de novos processos de negócios e novos sistemas de informática. A tentativa de implementar a segurança em sistemas antigos é muito cara e geralmente não funciona.

PLANEJAMENTO NA ÁREA DA INFORMÁTICA

O livro de ficção científica "Hitchhikers Guide to the Galaxy" tem como primeira regra:

NÃO ENTRE EM PÂNICO. Este é um bom conselho para a o planejamento na segurança da informática, também. Muitas organizações resistiram à idéia de investir em informática por causa da crença persistente e exagerada de que elas imediatamente serão assediadas pelos hackers e invasores.

Apesar da maior exposição e do maior número de invasores em potencial, a experiência e as ferramentas para construir defesas eficazes já se encontram disponíveis e estão sendo constantemente aperfeiçoadas. Com um planejamento eficaz e em tempo hábil, é possível responder rapidamente e de maneira adequada a qualquer ataque, evitando a maior parte dos ataques e amenizando o impacto dos demais.

O planejamento geral de informática deve ser feito com uma visão bem ampla: o plano de informática deve fluir diretamente dos planos operacionais da organização. O plano deve descrever os requisitos de negócios que deverão possibilitar o atingimento das metas operacionais: ele não é uma lista de desejos de informática. Enfatize o que precisa ser feito e não como vai ser feito. Geralmente existem muitas maneiras de preencher um requisito com grandes diferenças de custo. Deve haver uma justificativa clara para cada dólar gasto. E a segurança deve ser parte do plano de informática desde o início.

As arquiteturas devem ser simples e devem continuar assim. Isso proporciona uma vantagem em termos de segurança. Os sistemas múltiplos, não importa o quão proximamente integrados forem, sempre oferecem muitos pontos de acesso e requerem sistemas de administração e suporte com níveis múltiplos de segurança, o que significa custos mais elevados.

SETE ESTRATÉGIAS PARA ASSEGURAR A SEGURANÇA NA ÁREA DE INFORMÁTICA

1. ANTES DE MAIS NADA — MANTENHA TUDO MUITO SIMPLES. Se o sistema for complicado demais, os usuários o evitarão ou tentarão contorná-lo; isso compromete a segurança e reduz a sua utilidade. As medidas de segurança modernas podem ser eficazes e discretas.
.
2. DESENVOLVA POLÍTICAS, PROCEDIMENTOS, E PENALIDADES (P3) ANTECIPADAMENTE. Projete P3 de segurança baseados nas necessidades dos usuários, na natureza dos aplicativos, e nas informações que estão sendo protegidas. CUMPRA-OS de maneira consistente. Ter P3 "mansos" é pior do que não ter nenhum.

3. PROPORCIONE TREINAMENTO NO USO DO SISTEMA E ENFATIZE OS P3. Reafirme o treinamento, revendo e distribuindo notícias relevantes — por exemplo, histórias referentes a ataques cibernéticos ou abusos de sistemas.

4. USE PRODUTOS DE SEGURANÇA DISPONÍVEIS, "COMUNS", EM VEZ DE DESENVOLVER APLICATIVOS DE SEGURANÇA INTERNAMENTE. Isso é aconselhável por vários motivos, porque as necessidades de negócios são relativamente simples. Os órgãos de justiça criminal associam pessoas a outras pessoas, e pessoas a eventos, colhendo e compartilhando informações. Os produtos comuns baseados em padrões abertos foram testados e provados; seus usuários podem ser entrevistados e você pode aprender alguma coisa com eles. Mesmo no caso de os produtos serem novos, as metodologias usadas nos testes podem ser avaliadas e os resultados, revistos. E o que é mais importante, os produtos padrão da indústria geralmente são bem documentados, para o usuário e para o pessoal técnico da área técnica de informática. A documentação e os testes quanto à segurança são freqüentemente relegados ao segundo plano quando se desenvolve aplicativos internamente.

5. COMPARTIMENTALIZE AS INFORMAÇÕES, ATIVOS E USUÁRIOS. PROTEJA AS INFORMAÇÕES E ATIVOS ADEQUADAMENTE DE ACORDO COM O SEU VALOR. Os relatórios de inteligência de natureza confidencial devem ser

muito bem guardados. As informações que forem públicas e/ou que possam ser facilmente substituídas, no entanto, não requerem uma segurança muito sofisticada. Uma avaliação objetiva dos ativos de informação revelará que os itens públicos ocorrem com muito mais freqüência do que os confidenciais.

Da mesma fora, os ativos de informática (PCs, cabos, hubs, etc.) e suprimentos (software, disquetes, etc.) devem ser adequadamente inventariados e protegidos. Freqüentemente, os órgãos públicos recebem grandes quantidades de hardware e software (PCs, monitores, placas de rede, hubs, roteadores, etc.) sem lançar os itens em um banco de dados de controle de ativos, e sem verificá-los cuidadosamente para se assegurar de que eles são o que foi encomendado e que os itens estão configurados adequadamente e funcionando perfeitamente. Quando os itens são perdidos ou não funcionam adequadamente, não existe um registro para provar que a perda ocorreu ou que o sistema não está apresentando o desempenho que dele se espera. O gerenciamento de inventário é a primeira providência a ser tomada. A segunda é o controle de configuração.

Por ocasião da entrega, a configuração de cada item de hardware deve ser ajustada e cada item de software deve ser adequadamente inventariado. O inventário, portanto, conterá uma descrição detalhada de todos os componentes do sistema, hardware, e software, e onde eles estão localizados (incluindo o número da sala e a mesa). Essas informações são de valor inestimável na proteção dos ativos, na identificação de roubo e adulteração, e na realização de investigações eficazes quando forem detectados problemas. Existem programas de computador disponíveis no mercado que verificam a configuração e informam a ocorrência de problemas aos administradores de segurança automaticamente. Esses programas também mantêm um registro das modificações e da manutenção do sistema. À medida que os reparos ou atualizações são feitos nos sistemas e que a manutenção é realizada, é importante que haja um registro de tais atividades. Finalmente, travas e parafusos especiais para selar as estações de trabalho podem reduzir o número de ocorrências de roubo ou adulteração. A política da organização deve exigir que todos os problemas dos quais se suspeite sejam relatados para que possam ser investigados.

A compartimentalização de suprimentos e ativos significa tratá-los mais adequadamente de acordo com o seu custo ou a sua importância para a missão. Essa área freqüentemente é negligenciada. Por exemplo, os órgãos governamentais mantêm suprimentos baratos como disquetes em armários trancados, enquanto ativos críticos como um servidor ficam desprotegidos em uma área aberta do escritório, e cabos e hubs de rede passam por paredes abertas em vez de serem protegidos por condutos e ocultos no teto.

Compartimentalize os usuários também. Controle os aplicativos e as informações aos quais os usuários têm acesso e a maneira pela qual esse acesso é feito. (Por exemplo, um usuário pode ter permissão para acessar um arquivo restrito somente de uma certa estação de trabalho, em certas ocasiões). Controle as pessoas que podem criar contas ou identificações de usuários em um sistema. Conduza auditorias freqüentemente para ver se há identificações ou contas sem dono.

Tenha uma boa capacidade instalada para a realização de auditorias.

Uma das ameaças à segurança que é ignorada com a maior frequência é a documentação dos sistemas. Documentos de todos os tipos freqüentemente são tratados de forma demasiadamente casual e podem ser encontrados abertos em escritórios que não apresentam nenhuma segurança. As informações detalhadas de conteúdo técnico, ou que se destinem aos usuários, devem ser protegidas. Pode parecer conveniente e mais barato preparar e publicar um único tipo de documentação que sirva para todos, mas isso pode ser perigoso para a segurança do sistema. Manuais para os usuários finais, que são distribuídos em grandes quantidades freqüentemente contêm muitas informações técnicas que são inúteis para o usuário, mas que são muito valiosas para um hacker. Um hacker armado com informações detalhadas sobre o sistema pode atacar um sistema com precisão cirúrgica em vez de apelar para os ataques de força bruta, cuja detecção é mais fácil. Distribua a documentação de acordo com a necessidade de cada um. Quem não precisa saber o conteúdo da documentação não deve recebê-la.

Proteja a documentação, controle o acesso a ela, e treine os usuários sobre a maneira de protegê-la. A publicação de documentos na rede em vez de fazê-lo na forma de

documentos impressos é recomendada para reduzir os custos, simplificar as atualizações, e proporcionar maior proteção.

6. SEJA REALISTA QUANTO À ADMINISTRAÇÃO DA SEGURANÇA. É pouco provável que os órgãos de justiça criminal, por exemplo, possam estabelecer ou administrar um programa de segurança de informática que seja impenetrável. Estabeleça um equilíbrio entre as reais necessidades de segurança e os custos da segurança. Talvez seja possível contratar o nível desejado de suporte para atingir os mesmos objetivos. Use os funcionários da organização para fazer o que eles realmente podem fazer de maneira mais eficaz, e terceirize ou "redistribua" o resto. A principal coisa a ser feita é obter os resultados definidos pelo plano de segurança de informação.

Muitos recursos se encontram disponíveis para atender às necessidades de segurança. Eles podem ser terceirizados para uma empresa privada a custos competitivos. À medida que a dependência da informática aumenta e a segurança passa a assumir uma importância maior, as empresas estão respondendo, oferecendo serviços de segurança em informática de alta qualidade.

Além disso, vale a pena "redistribuir" serviços. A redistribuição descreve o que os órgãos de justiça criminal e membros da comunidade de segurança podem fazer uns pelos outros. A partilha de recursos, as aquisições conjuntas feitas com dinheiro recolhido de vários órgãos, os serviços prestados gratuitamente por universidades ou pela comunidade — todas essas coisas são maneiras pelas quais se pode eliminar os hiatos no plano de segurança.

7. TESTE, AUDITE, INSPECIONE SITES E INVESTIGUE DE MANEIRA CONTÍNUA E ALEATÓRIA. Use uma metodologia para analisar e testar código para bloquear as "portas dos fundos" dos sistemas. Use programas automatizados de auditoria e monitoração. Use programas que verifiquem as mudanças ocorridas em um arquivo. Desenvolva e use programas de "dicas" como uma forma de identificar atacantes existentes ou possíveis dos sistemas. Divulgue ameaças e respostas a eles. Sempre tome medidas rapidamente, de maneira consistente e apropriada quando as violações forem detectadas ou relatadas. Anuncie amplamente as punições ocorridas nos casos de segurança de informática.

TECNOLOGIAS EMERGENTES

A segurança na área de informática tem progredido tão rapidamente quanto todos os outros aspectos da informática, mas ela não pode ser eficaz se não for adequadamente aplicada. Características de segurança se encontram disponíveis em quase todos os aplicativos comerciais de uso comum. Atualmente, as paredes de proteção (firewalls) estão mais poderosas e adaptáveis do que nunca e se encontram disponíveis a preços realistas. Os programas de criptografia estão se tornando muito mais poderosos e mais fáceis de implementar e manter. A capacidade de administrar e monitorar sistemas distribuídos, de um único ponto na rede, está sendo constantemente aperfeiçoada. Os programas automatizados de monitoramento e auditoria, para controlar o uso do sistema e alertar os administradores de segurança em caso de tentativas de abusos, estão se tornando mais amadurecidos rapidamente.

Uma das áreas mais promissoras no que se refere ao progresso técnico é a biometria — a capacidade de identificar alguém tendo com base uma característica exclusiva (por exemplo, impressão digital, voz, geometria das mãos, padrão de retina, etc.). Os dispositivos biométricos fazem com que seja possível autenticar usuários com uma eficácia sem precedentes e impedem as pessoas não autorizadas de acessar um sistema, mesmo se elas possuírem uma senha.

A IBM, em colaboração com o Banco Barclays, na Europa, está testando teclados de estações de trabalho com uma leitora de impressões digitais embutida. Os usuários precisam ser biometricamente autenticados antes de poderem ter acesso a qualquer parte do sistema. A tecnologia de "flash" (um algoritmo de busca de imagens) é rápida e precisa. Ela pode fazer uma busca em um banco de dados de milhões de registros (incluindo imagens de impressões digitais) para determinar se os registros coincidem. Essa capacidade, combinada com redes de alta velocidade, tem um grande potencial para uso em ATMs (caixas automáticas de bancos) e outros dispositivos usados para transações eletrônicas. A tecnologia de flash está sendo usada em um sistema, baseado em impressões

digitais, de verificação de registros de eleitores no Peru. O projeto tem apresentado excelentes resultados e ajudará a impedir as fraudes eleitorais.

À medida que essas tecnologias continuam a evoluir, a segurança na informática continuará a melhorar em termos de eficácia e facilidade de uso.

A GUERRA DA INFORMAÇÃO: DESAFIO E OPORTUNIDADE

James Adams
Diretor Geral, Infrastructure Defense, Inc.

"Sentado na minha casa, com o meu computador e o meu modem, eu tenho o poder e a capacidade...de fazer guerra," diz James Adams. "Trata-se de um ambiente muito diferente de qualquer coisa que já tenhamos experimentado no passado." Adams é o diretor geral da Infrastructure Defense, Inc., que proporciona um espaço para a troca de informações e tomada de decisões sobre a infra-estrutura crítica no setor privado e entre os setores público e privado em âmbito mundial. Este artigo é uma adaptação das declarações feitas por Adams na Agência de Informações dos Estados Unidos em agosto de 1998.

No ano passado, as forças armadas dos Estados Unidos organizaram um exercício que envolvia uma simulação na qual uma crise internacional estava em andamento e um governo estrangeiro havia contratado 35 hackers de computador para neutralizar a reação dos Estados Unidos àquela crise. Os "hackers" que estavam participando do exercício — chamado Eligible Receiver [Receptor Autorizado] — eram, na verdade, funcionários do governo dos Estados Unidos. Eles não receberam nenhuma informação prévia. Eles compraram os seus laptops em uma loja local de artigos de informática.

Os hackers foram bem sucedidos na sua demonstração de que podiam facilmente penetrar nas malhas energéticas de todas as principais cidades dos Estados Unidos -- de Los Angeles a Chicago, a Washington, D.C., ou a Nova York — que estavam ligadas à capacidade dos Estados Unidos de posicionar forças. Ao mesmo tempo eles conseguiram penetrar no sistema de telefonia de emergência "911" e poderiam, facilmente, ter tirado as duas redes do ar.

Em seguida eles acessaram o sistema de comando e controle do Pentágono. Em poucos dias eles interrogaram 40.000 redes e obtiveram acesso, no nível inferior, a 36 delas. Eles conseguiram penetrar profundamente na estrutura de comando e controle, e se quisessem, poderiam ter impedido aquela estrutura de funcionar de maneira eficaz.

O que este exercício demonstrou é que 35 pessoas, usando informações disponíveis publicamente, com habilidades que se encontravam disponíveis no mundo inteiro, podiam ter impedido os Estados Unidos de responder a uma crise.

Trata-se de uma extraordinária demonstração da força que a guerra da informação representa. Essa força obrigou os Estados Unidos a investirem muito dinheiro no desenvolvimento de uma capacidade ofensiva eficaz onde a guerra pode ser conduzida por outros meios.

Para os que possuem a capacidade, aí está a oportunidade de fazer a guerra — não posicionando soldados, da forma convencional em um campo de batalha, onde muitos milhares deles morreriam, ou, até mesmo posicionando mísseis da forma convencional — mas em vez disso, lançando pelo espaço cibernético, bits e bytes, que destróem com eficácia um agressor em potencial antes de as tropas se encontrarem no campo de batalha.

Isso significa apagar as luzes de uma grande cidade. Isso significa impedir os mercados financeiros internacionais de funcionar adequadamente. Isso significa interromper o fluxo de informações em um país estrangeiro, e inserir o fluxo de informações do atacante, de modo que seja possível efetuar operações psicológicas muito eficazes contra um inimigo em potencial.

Essas coisas parecem bastante brandas, mas na verdade elas podem causar o tipo de perda de vidas que uma grande campanha de bombardeio também pode infligir.

Por exemplo, um estudo feito pela Força Aérea dos Estados Unidos sobre as conseqüências de se nocautear a malha energética da região sudoeste dos Estados

Unidos demonstrou que 20.000 pessoas teriam morrido. Isso teria um efeito devastador na moral do país e apresentaria desafios novos e muito interessantes sobre a maneira pela qual reagiríamos.

No drama com o Iraque poucos meses atrás, enquanto nos preparávamos para a possibilidade de agir militarmente, foi detectado um esforço no sentido de interferir com a rede de logística dos Estados Unidos. Descobriu-se, posteriormente, que a origem desse esforço era um prédio em Abu Dhabi. Assumiu-se que o líder iraquiano Saddam Hussein estava conduzindo uma guerra de informação contra os Estados Unidos, antes do início da operação militar. Americanos foram posicionados para lidar com essa ameaça. Ao chegar ao prédio em questão, eles descobriram um roteador (um ponto de transferência) na Internet, e na verdade, o "ataque" estava sendo lançado por alguns adolescentes nos Estados Unidos.

Essa é uma clara demonstração do verdadeiro desafio e da oportunidade que a guerra de informação apresenta. Podemos lançar um ataque, e podemos dar a impressão de que ele vem de algum lugar bem distante do seu real ponto de origem. Da mesma forma, quando um ataque é lançado contra nós, é muito, muito difícil, descobrir de onde ele vem. Mesmo se você descobrir a fonte, é muito difícil, nesse momento, lançar um ataque. O que você está atacando e por que você está fazendo isso? Qual será a resposta do público e o apoio do público, para as suas ações, se milhares de pessoas morrerem? Como você consegue persuadir as pessoas de que esta era a coisa certa a fazer? Não há provas — não podemos mencionar bebês mortos nas ruas. Não há nenhum homem de pé, em uma esquina, empunhando uma arma. Não se trata do tipo da coisa com a qual as pessoas estão acostumadas. Isso apresenta um verdadeiro desafio.

Essas questões e as oportunidades que elas representam estão se tornando muito atraentes para quase todos os países que possuem capacidade de realizar operações na área da informática. Para a nação-estado, o potencial da guerra de informação é uma coisa atraente, mas também é extremamente ameaçador, porque a guerra da informação não trata de nações; ela trata do poder que é atribuído aos indivíduos.

Eu acredito que a guerra da informação está, fundamentalmente, mudando uma dinâmica que existe há muito tempo, que ajudou a manter a estabilidade entre os estados, isto é, o governo decide o ritmo da mudança, de modo geral, e é um instrumento para uma boa parte dessas mudanças.

Quando um novo sistema de armamento é desenvolvido, leva muito tempo até que esse sistema de armamento vá, do país que o gerou, para um país que não tem a capacidade de produzi-lo. Vamos falar de um ciclo de 20 anos. Hoje, o mais recente computador é desenvolvido pela Compaq, possui software fornecido pela Microsoft, e se encontra disponível na CompUSA, uma loja de artigos de informática com filiais em todo o território dos Estados Unidos. Pode ser — ressaltamos o "pode ser" — que o governo o compre dentre dos próximos dois ou três anos, mas isso é muito pouco provável. Entretanto, eu posso ir até a loja de informática com o meu talão de cheques na mão e comprá-lo. Em uma guerra de informação, essa é a minha arma.

Sentado na minha casa, com o meu computador e o meu modem, eu tenho o poder e a capacidade...de fazer guerra — isto é, se eu soubesse fazer isso. Trata-se de um ambiente muito diferente de qualquer coisa que já tenhamos experimentado no passado.

O que é particularmente interessante, eu acho, é que o que estamos vendo enquanto essa revolução na informação se desencadeia — e nós ainda estamos no comecinho dela — é a nova gama de alianças que está surgindo. Recentemente eu falei com um amigo que montou uma conferência on-line de montanheses. Trata-se de pessoas que vivem nas montanhas em todas as partes do mundo — sejam elas nos Alpes, ou nos Urais, ou nas Rochosas ou em qualquer outro lugar — e eles tiveram uma conferência on-line de dois dias. Essas pessoas, que nunca haviam se comunicado antes, descobriram que tinham muita coisa em comum. Todas elas detestavam as pessoas que viviam no vale. Todas elas odiavam o governo e todas elas se importavam, de maneira apaixonada, com meio ambiente.

Esse é um exemplo de uma nova comunidade cujos membros têm mais coisas em comum um com o outro do que eles têm, talvez, com os outros cidadãos das nações em que eles, de fato, vivem. Agora todos esses grupos — sejam eles as 52 organizações terroristas que,

no momento, possuem sites na Web, organizações ambientalistas, ou pessoas que simplesmente se sentem excluídas — têm uma oportunidade de se comunicar, de compartilhar conhecimentos, e de expressar suas frustrações. É impressionante como há uma unidade — ou uma capacidade de se unir — nesses grupos que nunca haviam existido.

Embora nós não tenhamos a capacidade de eliminar a probabilidade de uma guerra, nós temos a capacidade ofensiva de fazer guerra por outros meios e certamente mudar a maneira pela qual chegamos ao conflito tradicional. E isso traz alguns desafios de verdade. Antes de mais nada, o governo precisa entender o que a guerra significa. Ainda estamos presos em um ambiente de Guerra Fria. Se você perguntar à Força Aérea ou à Marinha, ou aos outros que estão desenvolvendo essa capacidade, "Quando você tem autorização para usar o que você tem?" eles dizem, "Bem, nós fizemos essa pergunta ao Departamento de Justiça uns dois anos atrás, e até agora eles ainda não responderam."

Trata-se de uma questão importante. Estas armas são projetadas para serem usadas exatamente antes de entrarmos em guerra, para impedir que entremos em guerra no sentido tradicional. E no entanto elas são muito agressivas e muito poderosas. Este vai sei um grande desafio para o governo. Na verdade, já é. Como é que o governo vai continuar tendo alguma importância quando tudo ao seu redor está mudando a um ritmo tão rápido?

Nos também, de uma maneira defensiva, temos que lidar com um tipo diferente de ameaça. Tradicionalmente as forças armadas se vêem como os soldados que vão até a linha de frente, lutam, ficam feridos, morrem, ou voltam; eles são bem sucedidos ou falham. Mas no novo ambiente, todos nós, na verdade, estamos na linha de frente. A questão é: como vamos nos defender e nos proteger, e como somos protegidos pelo governo ou pelo setor privado? Somos parte do processo. Isso representa um ambiente muito diferente.

O problema dos computadores no ano 2000 (o bug do milênio) é uma excelente ilustração disso. Na verdade trata-se de uma questão social, assim como a guerra da informação é uma questão social. A guerra da informação é uma questão de interromper o fornecimento de água, cortar a energia elétrica, fazer com que as usinas de tratamento de esgoto entrem em colapso, nocautear os sistemas de caixas automáticas dos bancos, enfim, remover o tecido da vida.

A tarefa de lidar com a conversão do ano 2000 demonstrará a abrangência da interdependência das infra-estruturas críticas. Por enquanto nós não entendemos — nenhum de nós entende — por completo, até que ponto tudo o que fazemos está interligado. Se uma peça do quebra-cabeça cair, o resto do quebra-cabeça também fica fragmentado. Não se trata apenas de uma questão em nível nacional; é uma questão internacional.

Portanto, ao nos prepararmos para enfrentar os desafios da guerra da informação, temos que tratar, ao mesmo tempo, dos desafios do governo. O que isso significa neste novo ambiente? Temos que tratar do desafio à infra-estrutura crítica. Como vamos defender essas estruturas adequadamente?

Um elemento vital é o setor privado porque, atualmente, o setor privado é a locomotiva que está conduzindo todas as mudanças que se desencadeiam ao nosso redor. O governo tem que demonstrar a sua importância e assumir alguma forma de liderança neste ponto, a qual eu acho que está perceptivelmente ausente.

O setor privado pode articular muitas dessas coisas para se defender, e desta forma, para nos defender a todos. Se nós não reconhecermos isso, acho que vamos ter sérios problemas, a começar pelo bug do milênio. Nós nos tornaremos vítimas dos novos agressores que nos rodeiam, que terão um poder que nós ainda nem começamos a compreender e que quando compreendermos, será tarde demais.

O que eu gostaria de fazer é tentar educar as pessoas sobre essas questões e encorajar não apenas a conscientização do público, e sim mais ação por parte daqueles que têm a capacidade de divulgar os fatos, e assim criar defesas contra o que será um ambiente extremamente agressivo no próximo século.

FATOS E NÚMEROS: A PROTEÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS DOS EUA

(Determinação Presidencial N.º 63)

As informações que se seguem, a respeito da Determinação Presidencial N.º 63, foram divulgadas pela Casa Branca no dia 22 de maio de 1998.

Esta Determinação Presidencial se baseia nas recomendações da Comissão Presidencial Para a Proteção da Infra-Estrutura Crítica. Em outubro de 1997, a Comissão emitiu o seu relatório, solicitando que fosse feito um esforço, em nível nacional, para garantir a segurança das infra-estruturas dos Estados Unidos, que são cada vez mais vulneráveis e inter-conectadas, como ocorre com as telecomunicações, sistemas bancário e financeiro, energia, transportes, e serviços essenciais do governo.

A Determinação Presidencial 63 é o resultado de um esforço intenso, de vários órgãos governamentais, para avaliar essas recomendações e produzir uma estrutura prática e inovadora para a proteção da infra-estrutura crítica. A política do presidente:

— Estabelece como objetivo uma infra-estrutura de informática confiável, inter-conectada, e segura até o ano 2003, e aperfeiçoamentos significativos na segurança dos sistemas do governo até o ano 2000, pelos meios descritos a seguir:

  a) Criação imediata de um centro nacional para alerta e reação a ataques.
  b) Construção da capacidade de proteger infra-estruturas críticas contra atos intencionais até 2003.

— Aborda as vulnerabilidades das infra-estruturas cibernéticas e físicas do governo federal, determinando que cada departamento e órgão governamental trabalhe no sentido de reduzir a sua exposição a novas ameaças;

— Requer que o governo federal sirva como modelo para o resto do país, no que se refere à maneira pela qual a infra-estrutura deve ser protegida;

— Procura a participação voluntária das empresas privadas no atingimento de metas comuns para a proteção dos nossos sistemas críticos, por meio de parcerias entre os setores público e privado;

— Protege os direitos à privacidade e procura utilizar as forças de mercado. Tem como objetivo fortalecer e proteger o poder econômico da nação, e não sufocá-lo.

— Busca a total participação e contribuição por parte do Congresso.

A PDD-63 estabelece uma nova estrutura para lidar com este importante desafio:

— Um Coordenador Nacional cujas atribuições incluirão não somente a infra-estrutura crítica, mas também o terrorismo internacional e as ameaças de destruição em massa em nível nacional (incluindo armas biológicas) porque os ataques aos Estados Unidos podem não ser rotulados e embalados de maneira sistemática, em diferentes jurisdições;

— O Centro Nacional de Proteção da Infra-Estrutura [National Infrastructure Protection Center], na polícia federal [Federal Bureau of Investigation], reunirá representantes do FBI, do Departamento de Defesa, do Serviço Secreto dos Estados Unidos, dos Departamentos de Energia e dos Transportes, da Comunidade de Inteligência, e do setor privado, em uma tentativa sem precedentes de compartilhar informações entre órgãos governamentais em colaboração com o setor privado. Além disso o Centro proverá os principais meios para facilitar e coordenar a resposta do governo federal a um incidente, minimizando os efeitos dos ataques, investigando ameaças, e monitorando o trabalho de reconstrução;

— O setor privado é incentivado a estabelecer um Centro de Troca e Análise de Informações [Information Sharing and Analysis Center], em colaboração com o governo federal;

— Um Conselho Nacional de Garantia da Infra-Estrutura [National Infrastructure Assurance Council] formado a partir das lideranças do setor privado e autoridades dos governos estaduais e municipais, para proporcionar orientação para a formulação da política de um Plano Nacional;

— O Escritório Para a Garantia da Infra-Estrutura Crítica [Critical Infrastructure Assurance Office] proporcionará apoio ao trabalho do Coordenador Nacional com os órgãos governamentais e com o setor privado, durante o desenvolvimento de um plano nacional. Além disso, o escritório ajudará a coordenar um programa nacional de educação e conscientização, e de relações com o legislativo e com a comunidade.

Para maiores informações sobre esta Determinação Presidencial, entre em contato com o Escritório Para a Garantia da Infra-Estrutura Crítica, pelo telefone (703) 696-9395 e solicite cópias do White Paper on Critical Infrastructure Protection [Relatório Sobre a Proteção da Infra-Estrutura Crítica]. ◉

A Ameaça Cibernética: Protegendo as Redes de Informação dos EUA
NOTIFICAÇÃO SOBRE ARTIGOS

Bennett, Robert, et al. THE Y2K CRISIS: A GLOBAL TICKING TIME BOMB? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 147-166)
Consultores da área de administração, indivíduos encarregados de fazer planejamento financeiro, e peritos nas questões de conversão do ano 2000 alertam, em cinco ensaios, que o problema de computadores no ano 2000 merece ser levado a sério – e logo, antes que seja tarde demais. O senador Bennet, que lidera um Comitê Especial do Senado a respeito do problema da conversão do ano 2000, diz que o "maior desafio" é "fazer com que as pessoas pensem...transcendendo os limites individuais das nossas próprias organizações, e na verdade, transcendendo os limites das fronteiras do nosso país." E "devemos...reconhecer que não se trata de um problema de informática" e sim "um desafio gerencial", que deve ser tratado imediatamente nos mais altos níveis, ele diz.

Bowers, Stephen R. INFORMATION WARFARE: THE COMPUTER REVOLUTION IS ALTERING HOW FUTURE WARS WILL BE CONDUCTED (Armed Forces Journal International, August 1998, pp. 38-39)
Argumentando que o acesso à informação na atualidade é tão crucial quanto a posse de petróleo e munição, Bowers discute a ameaça representada por "atacantes a computadores que são quase invisíveis" para as malhas energéticas, redes de transportes, sistemas financeiros, e sistemas de telefonia de uma nação. Ele diz que exercícios recentes, conduzidos pelas forças armadas dos Estados Unidos, envolveram ações que elevam a guerra da informação do nível tático para o nível estratégico. A guerra da informação envolve um novo tipo de campo de batalha, mas com o potencial de causar um número igualmente elevado de baixas, ele diz.

Gompert, David C. NATIONAL SECURITY IN THE INFORMATION AGE (Naval War College Review, vol. 51, no. 4, sequence 364, Autumn 1998, pp. 22-41)
Gompert, diretor do Instituto Nacional de Pesquisas de Defesa [National Defense Research Institute] na RAND, argumenta que as mudanças causadas pelas revolução na área da informática trouxeram grandes benefícios para os Estados Unidos, embora tenham trazido problemas também. A revolução da informática expandiu a liberdade econômica e política, Gompert diz, expandindo a "base democrática" do mundo. Ela trouxe mudanças significativas na conduta da guerra, dando aos Estados Unidos, com a sua liderança na tecnologia de informação, uma grande vantagem: "Falando de uma maneira simplificada, a informática pode ajudar os que a dominam a vencer grandes guerras a grandes distâncias, com pequenas forças," diz Gompert. Ele cita uma preocupação no sentido de que as nações não-confiáveis "provavelmente apelarão para estratégias assimétricas, como por exemplo, ataques com armas de destruição em massa, terrorismo e guerra de informação contra os Estados Unidos e seus parceiros."

Henry, Ryan; Peartree, C. Edward. MILITARY THEORY AND INFORMATION WARFARE (Parameters, vol. 28, no. 3, Autumn 1998, pp. 121-135)
Gompert, diretor do Instituto Nacional de Pesquisas de Defesa [National Defense Research Institute] na RAND, argumenta que as mudanças causadas pelas revolução na área da informática trouxeram grandes benefícios para os Estados Unidos, embora tenham trazido problemas também. A revolução da informática expandiu a liberdade econômica e política, Gompert diz, expandindo a "base democrática" do mundo. Ela trouxe mudanças significativas na conduta da guerra, dando aos Estados Unidos, com a sua liderança na tecnologia de informação, uma grande vantagem: "Falando de uma maneira simplificada, a informática pode ajudar os que a dominam a vencer grandes guerras a grandes distâncias, com pequenas forças," diz Gompert. Ele cita uma preocupação no sentido de que as nações não-confiáveis "provavelmente apelarão para estratégias assimétricas, como por exemplo, ataques com armas de destruição em massa, terrorismo e guerra de informação contra os Estados Unidos e seus parceiros."

Selden, Zachary. MICROCHIPS AND THE MILLENNIUM: THE NATIONAL SECURITY IMPLICATIONS OF THE YEAR 2000 PROBLEM (National Security Studies Quarterly, vol. 4, issue 3, Summer 1998, pp. 71-77)
Selden prevê que a maior parte dos programas de computadores associados com o problema do ano 2000 serão reparados ou descartados e que a maior parte dos chips de computador embutidos terão sido substituídos até 1º de janeiro de 2000. Os que permanecerem podem causar falhas imprevisíveis ou semear confusão suficiente

para permitir que estados ou terroristas conduzam ataques ou invasões secretos, ele diz. Os atores internacionais podem procurar se beneficiar de uma situação confusa nos Estados Unidos, na virada do milênio, o autor alerta, e alguns atuais pontos de fulgor em nível regional podem irromper em uma espiral de conflitos por causa da falha de sistemas." Sob uma perspectiva de segurança nacional, o problema "é a percepção de que o bug do milênio apresenta uma janela de vulnerabilidade", o autor diz.

Os comentários acima fazem parte de uma Notificação de Artigos mais abrangente que aparece na home page do Serviço de Informações dos Estados Unidos:
"http://www.usia.gov/admin/001/wwwhapub.html". ◉

A Ameaça Cibernética: Protegendo as Redes de Informação dos EUA
BIBLIOGRAFIA

Adams, James. THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE. New York: Simon & Schuster, 1998. 366p.

Arquilla, John; Ronfeldt, David F. (Editors). IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE. Santa Monica, CA: Rand, 1997. 501p.

Barnett, Roger W. INFORMATION OPERATIONS, DETERRENCE, AND THE USE OF FORCE (Naval War College Review, vol. 51, no. 2, Spring 1998, pp. 7-19)

Browne, J.P.R.; Thurbon, M.T. ELECTRONIC WARFARE, Vol. 4 of Brassey's Air Power: Aircraft Weapons Systems and Technology Series. Washington: Brassey's, 1998. 341p.

Cillufo, Frank J.; Tomarchio, Thomas. RESPONDING TO NEW TERRORIST THREATS (Orbis, vol. 42, no. 3, Summer 1998, pp. 439-452)

Clinton, William J. COMMENCEMENT ADDRESS AT THE UNITED STATES NAVAL ACADEMY IN ANNAPOLIS, MARYLAND (Weekly Compilation of Presidential Documents, vol. 34, no. 21, May 22, 1998, pp. 944-948)

Copley, Gregory R. RE-DEFINING PSYCHOLOGICAL STRATEGY IN THE AGE OF INFORMATION WARFARE (Defense & Foreign Affairs Strategic Policy, vol. 26, no. 6, June 1998, pp. 5-8)

Gunther, Christopher. YOU CALL THIS A REVOLUTION? (Foreign Service Journal, vol. 75, no. 9, September 1998, pp. 18-23)

Henry, Ryan; Peartree, C. Edward (Editors). INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Significant Issues Series, vol. 20, no. 1). Washington: Center for Strategic & International Studies, 1998. 216p.

Libicki, Martin C. INFORMATION WAR, INFORMATION PEACE (Journal of International Affairs, vol. 51, no. 2, Spring 1998, pp. 411-428)

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR. Santa Monica, CA: Rand, 1996. 90p.

Petersen, John L.; Wheatley, Margaret; Kellner-Rogers, Myron. THE YEAR 2000: SOCIAL CHAOS OR SOCIAL TRANSFORMATION? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 129-146)

Pfaltzgraff, Robert L.; Schultz, Richard H. (Editors). WAR IN THE INFORMATION AGE: NEW CHALLENGE FOR U.S. SECURITY POLICY. Washington: Brassey's, 1997. 320p.

Rathmell, Andrew. INFORMATION WARFARE: USA TACKLES CYBERTHREAT (Jane's Intelligence Review Pointer, vol. 5, no. 9, September 1, 1998, p. 14)

Ryan, Stephen M. SHOULD U.S. PLEDGE NOT TO MAKE FIRST CYBERSTRIKE? (Government Computer News, vol. 17, no. 24, August 3, 1998, p. 32)

Sanz, Timothy L. INFORMATION-AGE WARFARE: A WORKING BIBLIOGRAPHY (Military Review, vol. 78, no. 2, March-April 1998, pp. 83-90)

U.S. Senate, Select Committee on Intelligence. CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES. Washington: Government Printing Office, 1998. 177p.

Verton, Daniel. DOD PREPS OFFICE FOR CYBERDEFENSE (Federal Computer Week, vol. 12, no. 23, July 13, 1998, pp. 1-2)

A Ameaça Cibernética: Protegendo as Redes de Informação dos EUA
PRINCIPAIS SITES NA INTERNET

Por favor observe que o USIS não assume nenhuma responsabilidade pelo conteúdo e nem pela disponibilidade dos recursos abaixo relacionados; essa responsabilidade é única e exclusivamente dos respectivos provedores.

Air Force Information Warfare Center
http://www.afiwc.aia.af.mil/

Center for High Assurance Computer Systems of the Naval Research Laboratory
http://www.itd.nrl.navy.mil/ITD/5540/main.html

Computer Security Technology Center, Lawrence Livermore National Laboratory, U.S. Department of Energy
http://ciac.llnl.gov/cstc/

Critical Infrastructure Assurance Office
http://www.ciao.gov/

Cyberspace Policy Institute at George Washington University
http://www.seas.gwu.edu/seas/institutes/cpi/

Defense Information Infrastructure
http://spider.osfl.disa.mil/dii/

Defense Policy on the Year 2000 Computer Conversion Issue
http://www.defenselink.mil/issues/y2k.html

Glossary of Information Warfare Terms
http://www.psycom.net/iwar.2.html

IBM Corporation: Secure Way
http://www.ibm.com/Security/

Information Systems Security Association
http://www.issa-intl.org/

Information Warfare Academic Group, Naval Postgraduate School
http://web.nps.navy.mil/~iwag/

Information Warfare and Information Security on the Web
http://www.fas.org/irp/wwwinfo.html

Information Warfare: Glossary
http://www.informatik.umu.se/%7Erwhit/IWGlossary.html

Information Warfare Research Center
http://www.terrorism.com/infowar/documents.html

InfoWar.Com
http://www.infowar.com/main.html

Infrastructure Defense, Inc.
http://206.132.10.154/idmarketsite/

Microsoft Corporation (Key Initiatives)
http://www.microsoft.com/

National Colloquium for Information Systems Security
http://www.infosec.jmu.edu/ncisse/

National Infrastructure Protection Center of the Federal Bureau of Investigation
http://www.fbi.gov/nipc/home.htm

National Institute of Standards and Technology (NIST)
http://csrc.nist.gov/

National Security Agency
http://www.nsa.gov:8080/

President's Council on Year 2000 Conversion
http://www.Y2K.gov/java/index.htm

School of Information Warfare and Strategy, National Defense University
http://www.ndu.edu/inss/act/iwscvr.html

Technology News: Governments Beat Terrorists To Net Weapons
http://www.techweb.com:80/wire/story/TWB19980922S0018

U.S. Senate, Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information
http://www.senate.gov/~judiciary/terrtest.htm

Year 2000 Conversion: U.S. Information Agency
http://www.usia.gov/topical/global/y2k/

POLÍTICA EXTERNA DOS EUA

AGENDA

VOLUME 3 REVISTA ELETRÔNICA DA AGÊNCIA DE INFORMAÇÕES DOS ESTADOS UNIDOS NÚMERO 4

A Ameaça Cibernética: Protegendo as Redes de Informações dos EUA

Novembro de 1998